PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-077999

(43)Date of publication of application : 15.03.2002

(51)Int.Cl. H04Q 7/38
H04L 12/28

(21)Application number : 2000-255840 (71)Applicant : TOSHIBA CORP

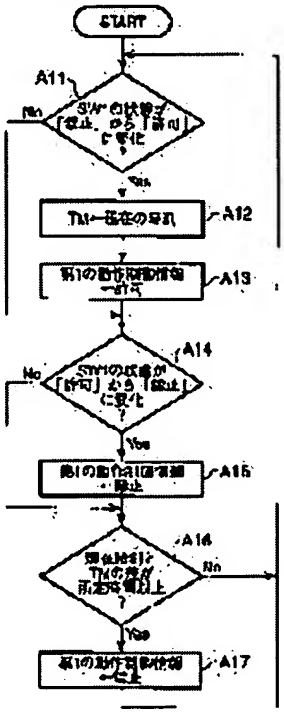
(22)Date of filing : 25.08.2000 (72)Inventor : ITO TAKAFUMI

(54) ELECTRONIC DEVICE AND CONNECTION CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To assure security by preventing unauthorized access from the other devices.

SOLUTION: When a switch is provided to a device body and this switch is switched to the acknowledgment condition, authentication by a particular recognition code (PIN code) is permitted (steps A1 to A13). When the switch is switched to the inhibition condition, authentication by the particular recognition code is inhibited (steps A14 and A15). Thereby, it can usually be prevented by setting the switch to the inhibition condition that a person makes an unauthorized access using the particular recognition code. Moreover, after the predetermined time has passed from the time when the switch is set to the acknowledgment condition, authentication by the particular recognition code is inhibited (steps A16 and A17). Accordingly, if it is forgotten that the switch is reset to the inhibition condition after the switch is set to the acknowledgment condition, security of device can be assured by preventing an unauthorized access.



LEGAL STATUS

[Date of request for examination] 25.08.2000

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3450808

[Date of registration] 11.07.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is electronic equipment equipped with the means of communications which requires authentication by specific identification code in case a link is stretched among other devices. The switch which can switch the 1st condition and 2nd condition, When this switch is set as the 1st condition Electronic equipment characterized by providing an authentication prohibition means to forbid authentication by the above-mentioned specific identification code, and an authentication authorization means to permit authentication by the above-mentioned specific identification code when the above-mentioned switch is set as the 2nd condition.
[Claim 2] Electronic equipment according to claim 1 characterized by providing the control means which forbids authentication by the above-mentioned specific identification code when having carried out predetermined time progress is detected, after the above-mentioned switch was set as the 2nd condition by time amount detection means to detect whether predetermined time progress was carried out after the above-mentioned switch was set as the 2nd condition, and this time amount detection means.
[Claim 3] A management information storage means to be electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices, and to memorize the various management information for connecting among other devices, When the switch which can switch the 1st condition and 2nd condition, and this switch are set as the 1st condition A modification prohibition means to forbid modification of the various management information memorized by the above-mentioned management information storage means, and when the above-mentioned switch is set as the 2nd condition Electronic equipment characterized by providing a modification authorization means to permit modification of the various management information memorized by the above-mentioned management information storage means.
[Claim 4] Electronic equipment according to claim 3 carry out having provided the control means which forbids modification of the various management information memorized by the above-mentioned management information storage means when having carried out predetermined-time progress was detected, after the above-mentioned switch was set as the 2nd condition by time-amount detection means detect whether predetermined time progress was carried out after the above-mentioned switch was set as the 2nd condition, and this time-amount detection means as the description.
[Claim 5] A device code storage means to be electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices, and to memorize the device code of each of other device by which the link was stretched, When there is a connection request from other devices and the device code of the device concerned is not memorized by the above-mentioned device code storage means When judged with an authentication error by authentication means to perform authentication by the above-mentioned specific identification code to the device concerned, and this authentication means An authentication error storage means to match and memorize the device code and the number of errors of the device concerned, Electronic equipment characterized by providing the control means which refuses the connection request from a device which

has the device code which corresponds when the number of errors memorized by this authentication error storage means exceeds the count of predetermined.
[Claim 6] An authentication means to be electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices, and to perform authentication by the above-mentioned specific identification code to the device concerned when there is a connection request from other devices, A link-information creation means to create a link information with the device judged as authentication being possible by this authentication means, A link-information registration means to match with an applicable device the link information created by this link-information creation means, and to register it, Electronic equipment characterized by providing a deletion means to delete the link information of the device judge that is unnecessary according to a predetermined regulation when the number of registered devices of the link information by this link-information registration means exceeds the permission number of cases.
[Claim 7] It is electronic equipment according to claim 6 which matches the above-mentioned link-information registration means with the link information of each of each device, memorizes both the last connection time of day of each of each device, and is characterized by the above-mentioned deletion means deleting the link information of the oldest device of the last connection time of day among the link informations registered into the above-mentioned link-information registration means.
[Claim 8] It is electronic equipment according to claim 6 which matches the above-mentioned link-information storage means with the link information of each of each device, memorizes the registration time of day both, and is characterized by the above-mentioned deletion means deleting the link information of the oldest device of the registration time of day among the link informations registered into the above-mentioned link-information registration means.
[Claim 9] It is electronic equipment according to claim 6 which matches the above-mentioned link-information storage means with the link information of each of each device, memorizes both the counts of connection of each of each device, and is characterized by the above-mentioned deletion means deleting the link information of fewest devices of the count of connection among the link informations registered into the above-mentioned link-information registration means.
[Claim 10] An identification code storage means to be electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices, and to memorize the above-mentioned specific identification code, An authentication means to perform authentication by the specific identification code memorized by the above-mentioned identification code storage means to the device concerned when there is a connection request from other devices, A link-information creation means to create a link information with the device judged as authentication being possible by this authentication means, A link-information registration means to match with an applicable device the link information created by this link-information creation means, and to register it, Electronic equipment characterized by providing a deletion means to delete all the link informations registered into the above-mentioned link-information registration means when the specific identification code memorized by the above-mentioned identification code storage means is changed.
[Claim 11] The exchangeable radio unit for being electronic equipment which requires authentication by specific identification code, in case a link is stretched among other devices, and connecting with a device besides the above, A unit code storage means to memorize the identification code of the proper of this radio unit, An authentication means to perform authentication by the above-mentioned specific identification code to the device concerned when there is a connection request from other devices, A link-information creation means to create a link information with the device judged as authentication being possible based on the identification code of the radio unit memorized by the above-mentioned unit code storage means with this authentication means, When exchanged for a link-information registration means to match with an applicable device the link information created by this link-information creation means, and to register it, in the above-mentioned radio unit Electronic equipment characterized by providing a deletion means to delete all the link informations registered into the above-mentioned link-information registration means.
[Claim 12] It is the connection control approach used for electronic equipment equipped with the means

of communications which requires authentication by specific identification code in case a link is stretched among other devices. When the switch which can switch the 1st condition and 2nd condition to the body of the above-mentioned electronic equipment is formed and this switch is set as the 1st condition The connection control approach characterized by permitting authentication by the above-mentioned specific identification code when authentication by the above-mentioned specific identification code is forbidden and the above-mentioned switch is set as the 2nd condition.
[Claim 13] The connection control approach according to claim 12 characterized by forbidding authentication by the above-mentioned specific identification code when predetermined time progress is carried out, after it judges whether it detected whether predetermined time progress was carried out after the above-mentioned switch is set as the 2nd condition, and the above-mentioned switch is set as the 2nd condition.
[Claim 14] It is the connection control approach used for electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices. It has the memory which memorized the various management information for connecting among other devices, and the switch which can switch the 1st condition and 2nd condition to the body of the above-mentioned electronic equipment is formed. The switch which can switch the 1st condition and 2nd condition, The connection control approach characterized by permitting modification of the various management information memorized by the above-mentioned memory when modification of the various management information memorized by the above-mentioned memory when this switch is set as the 1st condition is forbidden and the above-mentioned switch is set as the 2nd condition.
[Claim 15] The connection control approach according to claim 14 characterized by forbidding modification of the various management information memorized by the above-mentioned memory when predetermined time progress is carried out, after it judges whether predetermined time progress was carried out after the above-mentioned switch is set as the 2nd condition, and the above-mentioned switch is set as the 2nd condition.
[Claim 16] It is the connection control approach used for electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices. When the device code of each of other device by which the link was stretched is memorized in the 1st memory and there is a connection request from other devices When the device code of the device concerned is not memorized by the 1st memory of the above When authentication by the above-mentioned specific identification code is performed to the device concerned and it is judged with an authentication error according to this authentication The connection control approach characterized by refusing the connection request from a device which has the device code which corresponds when the number of errors which matched the device code and the number of errors of the device concerned, memorized in the 2nd memory, and was memorized by this 2nd memory exceeds the count of predetermined.
[Claim 17] It is the connection control approach used for electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices. When there is a connection request from other devices, authentication by the above-mentioned specific identification code is performed to the device concerned. A link information with the device judged as authentication being possible according to this authentication is created. The connection control approach characterized by deleting the link information of the device judge that is unnecessary according to a predetermined regulation when this link information is matched with an applicable device, it registers with memory and the number of registered devices of the link information by this memory exceeds the permission number of cases.
[Claim 18] It is the connection control approach used for electronic equipment equipped with a radio means to require authentication by specific identification code in case a link is stretched among other devices. Authentication by the specific identification code memorized to the device concerned by the 1st memory of the above when the above-mentioned specific identification code was memorized in the 1st memory and there was a connection request from other devices is performed. A link information with the device judged as authentication being possible according to this authentication is created. The

connection control approach characterized by deleting all the link informations that matched this link information with the applicable device, registered with the 2nd memory, and were registered into the 2nd memory of the above when the specific identification code memorized by the 1st memory of the above was changed.

[Claim 19] In case a link is stretched among other devices, authentication by specific identification code is required. It is the connection control approach of electronic equipment equipped with the exchangeable radio unit for connecting with a device besides the above. The identification code of the proper of the above-mentioned radio unit is memorized in the 1st memory. When there is a connection request from other devices, authentication by the above-mentioned specific identification code is performed to the device concerned. A link information with the device judged as authentication being possible is created based on the identification code of the radio unit memorized by the above-mentioned memory according to this authentication. The connection control approach characterized by deleting all the link informations registered into the 2nd memory of the above when this link information is matched with an applicable device, it registers with the 2nd memory and it is exchanged in the above-mentioned radio unit.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to electronic equipment and the connection control approach equipped with the radio function to perform data communication among other devices.
[0002]
[Description of the Prior Art] In recent years, the radio communications system of personal area, such as IrDA, Bluetooth, and HomeRF, attracts attention. It has the advantages, like that there is no directivity as compared with an infrared communication mode like IrDA, and especially Bluetooth and HomeRF have high permeability, and future development and spread are expected very much. In addition, Bluetooth is the radio specification of a short distance and realizes radio (less than 10m or less than 100m) using the ISM (Industrial Science Medical) band of a 2.4GHz band.
[0003] Connection with two or more devices is possible for radio communications systems, such as Bluetooth and HomeRF, to coincidence, and also it is one of the descriptions also with big a transmission distance being also comparatively as long as 10-100m as compared with an infrared communication mode like IrDA. Since there is also an advantage of improvement in user-friendliness but on the other hand this can be easily accessed from the outside by wireless, it fully needs to be careful about reservation of the security of a radio communications system, and unknown episode nature etc.
[0004] As a security method of a common radio communications system, the method indicated by the official report of patent No. 2872996 is learned. In the security system which consists of an electronic key and a wireless terminal unit, in order to strengthen security, this forbids the continuous duty of the same key and raises the safety to loss or a theft.
[0005] Moreover, in Bluetooth, the security method by the following user authentication is adopted.
[0006] The user authentication in Bluetooth is managed by two, the unique authentication password set as a device, and the cryptographic key created by ID (address which is 48 bits which IEEE manages and numbers) of this authentication password and a device proper etc. The above-mentioned authentication password is called the PIN (Personal Identification Number) code, and consists of character strings of arbitration. The above-mentioned cryptographic key is called a link key, and is used for a data encryption etc. other than user authentication.
[0007] Now, the case where Device A accesses to Device B is considered.
[0008] In the situation that Device A and Device B are connected for the first time, Device A needs to input the PIN code of Device B. When the PIN code inputted from Device A is judged to be the right, Device B establishes a link as authentication being possible, and permits connection. At this time, Device B multiplies a random number by the own PIN code and ID of Device A, creates the link key of Device A, and saves this on the link key table with ID of Device A. In addition, when creating a link key, ID of the PIN code of the partner who exchanges the link key of each other between each device, or self is also used.
[0009] On the other hand, if Device A may be connected to Device B before, since the link key of Device A is already registered into the above-mentioned link table, the input of the PIN code is excluded

and authentication by the above-mentioned link key is performed.
[0010]
[Problem(s) to be Solved by the Invention] There is what are various as a device using Bluetooth, and there is a line connection device called a modem access point as one of them. If this modem access point is equipped with the connect function to a public line and the communication facility of Bluetooth is added to this, it will become connectable by wireless among other devices corresponding to Bluetooth. Therefore, if a modem access point is accessed by wireless from an external instrument, in an external instrument side, without needing connection of a modular cable, it can connect with a public line and use of the Internet etc. can be received. In this case, authentication by the PIN code or link key mentioned above is carried out to access to a modem access point, and connection with a modem access point is allowed only for the external instrument judged as authentication being possible.
[0011] However, when known by persons other than the user of original [code / of a modem access point / PIN] in a certain means, it may access unlawfully to a modem access point using the PIN code. In the case of a modem access point, since a circuit toll arises by connection of a public line, unlawful access poses a serious problem.
[0012] Moreover, a modem access point is installed in the location which is not conspicuous, and the power source is usually always turned on in many cases. For this reason, before a manager knows, possibility of accessing unlawfully to a modem access point from the exterior is high.
[0013] It was made in order that this invention might solve the above points, and it aims at offering the electronic equipment and the connection control approach of being able to prevent unlawful access from other devices and securing security.
[0014]
[Means for Solving the Problem] namely, by the electronic equipment concerning claim 1 of this invention In case a link is stretched among other devices, when authentication by specific identification code is required and the switch which can switch the 1st condition and 2nd condition is set as the 1st condition When authentication by the above-mentioned specific identification code is forbidden and the above-mentioned switch is set as the 2nd condition Since authentication by the above-mentioned specific identification code is permitted, the user of other devices can stretch a link with the device concerned, unless it changes the setting actuation of the above-mentioned switch into the 1st condition, even if it knows the above-mentioned specific identification code.
[0015] Moreover, by the electronic equipment concerning claim 2 of this invention, since the authentication by the above-mentioned specific identification code is forbidden when having carried out predetermined time progress is detected, after being in the electronic equipment concerning said claim 1 and setting the above-mentioned switch as the 2nd condition, after predetermined time progress as the 2nd condition set [the above-mentioned switch] can stretch a link with other devices no longer.
[0016] moreover, by the electronic equipment concerning claim 3 of this invention It is what requires authentication by specific identification code in case a link is stretched among other devices by radio. When it has a management information storage means to memorize the various management information for connecting among other devices and the switch which can switch the 1st condition and 2nd condition is set as the 1st condition When modification of the various management information memorized by the above-mentioned management information storage means is forbidden and the above-mentioned switch is set as the 2nd condition Unless it changes the setting actuation of the above-mentioned switch into the 1st condition even if the inaccurate user of other devices can connect with this electronic equipment since modification of the various management information memorized by the above-mentioned management information storage means is permitted, modification actuation of the various management information for connection with a device besides the above can be performed.
[0017] moreover, by the electronic equipment concerning claim 4 of this invention After being in the electronic equipment concerning said claim 3 and setting the above-mentioned switch as the 2nd condition, when having carried out predetermined time progress is detected Since modification of the various management information memorized by the above-mentioned management information storage means is forbidden, after predetermined time progress as the 2nd condition set [the above-mentioned

switch] cannot perform modification actuation of the various management information for connection with a device besides the above, and becomes as [be / nothing].
[0018] moreover, by the electronic equipment concerning claim 5 of this invention It is what requires authentication by specific identification code in case a link is stretched among other devices by radio. When it has a device code storage means to memorize the device code of each of other device by which the link was stretched and there is a connection request from other devices When the device code of the device concerned is not memorized by said device code storage means When authentication by the above-mentioned specific identification code is performed to the device concerned and it is judged with an authentication error, the device code and the number of errors of the device concerned are matched, and an authentication error storage means memorizes. And since the connection request from a device which has a corresponding device code is refused when the number of errors memorized by this authentication error storage means exceeds the count of predetermined, it comes to be unable to perform the attempt of the unjust connection from the same device.
[0019] moreover, by the electronic equipment concerning claim 6 of this invention It is what requires authentication by specific identification code in case a link is stretched among other devices by radio. If authentication by the above-mentioned specific identification code is performed to the device concerned and it is judged with authentication being possible when there is a connection request from other devices, a link information with the device concerned will be created, and this created link information is matched with an applicable device, and is registered into a link-information registration means. and when the number of registered devices of the link information by this link-information registration means exceeds the permission number of cases The link information of the oldest device among the registration link information (for example, the last connection time of day) (claim 7), Or since the unnecessary link information of the link information (claim 8) of the oldest device of registration time of day or the link information (claim 9) of fewest devices of the count of connection is judged and deleted A link information with a new connection device will be replaced with the link information of the low device of connection possibility, and can be registered.
[0020] moreover, by the electronic equipment concerning claim 10 of this invention It is what requires authentication by specific identification code in case a link is stretched among other devices by radio. Authentication by the specific identification code memorized by the above-mentioned identification code storage means to the device concerned when it had an identification code storage means to memorize the above-mentioned specific identification code and there was a connection request from other devices is performed. If judged with authentication being possible, a link information with the device concerned will be created, and this created link information is matched with an applicable device, and is registered into a link-information registration means. And since all the link informations registered into the above-mentioned link-information registration means are deleted when the specific identification code memorized by the above-mentioned identification code storage means is changed, it can be prevented that a link is stretched among other devices after rewriting of the above-mentioned specific identification code by the user who does not know the new identification code concerned.
[0021] moreover, by the electronic equipment concerning claim 11 of this invention It is what requires authentication by specific identification code in case a link is stretched among other devices by radio. It has a unit code storage means to memorize the identification code of the proper of the exchangeable radio unit for connecting with a device besides the above, and this radio unit. When there is a connection request from other devices, authentication by the above-mentioned specific identification code is performed to the device concerned. If judged with authentication being possible, a link information with the device concerned will be created based on the identification code of the radio unit memorized by the above-mentioned unit code storage means, and this created link information is matched with an applicable device, and is registered into a link-information registration means. And since all the link informations registered into the above-mentioned link-information registration means are deleted when exchanged in the above-mentioned radio unit, if after exchange of the above-mentioned radio unit creates the link information based on the identification code of the unit proper and does not reregister it, it can stretch a link with other devices.

[0022]
[Embodiment of the Invention] Hereafter, 1 operation gestalt of this invention is explained with reference to a drawing.
[0023] Drawing 1 is the perspective view showing the appearance configuration of the radio communications system concerning 1 operation gestalt of this invention. The personal computer (a personal computer is called hereafter) 100 which performs radio between the line connection device (an access point is called hereafter) 10 equipped with the connect function of a public line and this access point 10 is shown by drawing 1 .
[0024] The access point 10 and the personal computer 100 are equipped with PC card (BT-PC card is called hereafter) 20 according to the radio specification of Bluetooth free [desorption] as a radio card. An access point 10 and a personal computer 100 are equipping with this BT-PC card 20, and the data communication by wireless of them becomes mutually possible.
[0025] A personal computer 100 is used as an external instrument which accesses an access point 10 here. The keyboard 112, the liquid crystal display panel 116, and the card slot 118 are formed in the body 114 of this personal computer 100.
[0026] It connects with a public line 11 through the modular cable 12, and an access point 10 carries out wireless transmission of the data inputted from the public line 11 at a personal computer 100 while transmitting the data by which wireless transmission was carried out from the personal computer 100 to a public line 11.
[0027] The configuration of an access point 10 is shown in drawing 2 thru/or drawing 6 .
[0028] The perspective view showing the condition that drawing 2 used the access point 10 with the decomposition perspective view of an access point 10, and drawing 3 used it in every length, the perspective view in which drawing 4 shows the tooth-back side of an access point 10, and drawing 5 are the perspective view showing the condition of having used the access point 10 by every side, and the perspective view showing the base side of an access point 10.
[0029] as shown in drawing 2 thru/or drawing 6 , the access point 10 was formed with synthetic resin etc. -- it has the rectangle-like body 14 of a device mostly. This body 14 of a device has front 14a which curved slightly, this front face, almost flat tooth-back 14b which countered, side-face 14c of the pair which counters and 14d of top faces, and base 14e. And base 14e and tooth-back 14b of the body 14 of a device constitute the 1st and 2nd installation side, respectively.
[0030] As shown in drawing 3 and drawing 4 , as the body 14 of a device is used as every length or it is shown in drawing 5 R> 5, the body 14 of a device can be used for an access point 10 as every width by laying tooth-back 14b in desktop superiors by laying base 14e in desktop superiors. Moreover, two engagement hollows 16 for hanging a pin, a hook, etc. are formed in tooth-back 14b, and the tooth back can use the body 14 of a device for it also as a wall type in the condition of having countered with the wall, by using these engagement hollows 16.
[0031] The electric power switch 18 of a push button type is formed in one side-face 14c of the body 14 of a device. The RS232C connector 22 and the AC adapter terminal 23 for power-source connection are formed in side-face 14c of another side. Moreover, as a display which shows the operating state of an access point 10, two or more LED24 is located in a line, and is prepared in front 14a of the body 14 of a device. as operating state -- for example, power-source ON (POWER), transmission (SD), and reception (RD) -- off-hook -- standby / active (STB/ACT) condition of (OH) and BT-PC card 20 mentioned later are displayed.
[0032] The transparence covering 15 which can be detached and attached freely, and the card slot 28 and eject button 30 of a card slot 26 which are mentioned later are prepared in 14d of top faces of the body 14 of a device. Moreover, two modular jacks 32 and the slide switches 34a and 34b of a right-and-left pair which can connect the modular cable 12 for connecting an access point 10 to a public line 11, and one rotary switch 35 are formed in base 14e so that drawing 6 may show.
[0033] The skirt-board section 36 is set up along with the periphery section by base 14e, and notching 37 is formed in the part. In case this skirt-board section 36 uses the body 14 of a device as every length, it functions as the leg. The modular cable 12 connected to the above-mentioned modular jack 32 is

pulled out outside through notching 37. Therefore, without the modular cable 12 becoming obstructive even when using the body 14 of a device as every length, where the modular cable 12 is connected to a modular jack 32, by the skirt-board section 36, it is stabilized and the body 14 of a device can be supported.

[0034] In the body 14 of a device, the card slot 26 which functions as an attaching part is formed, and opening of the card slot 28 of this card slot is carried out to 14d of top faces of the body of a device. And it can let a card slot 28 pass to this card slot 26, and it can be equipped with the BT-AC card 20 free [desorption].

[0035] Next, the configuration of BT-PC card 20 is explained.

[0036] Drawing 7 is the perspective view of BT-PC card 20, and drawing 8 R> 8 is the decomposition perspective view of BT-PC card 20.

[0037] As shown in drawing 7 and drawing 8 , BT-PC card 20 is equipped with the body 40 of a card based on the specification of PCMCIA, and the transceiver section 42 based on both BT specification projected from the end side of the body of a card. the body 40 of a card consists of synthetic resin -- it has the rectangle-like frame 43 mostly. This frame 43 is supporting the periphery section of the card substrate 44 within the body 40 of a card. The connector 45 was attached in the end of the card substrate 44, and the other end of a card substrate is projected from the body 40 of a card.

[0038] On top-face 44a, two or more electronic parts 46 are mounted one front face of the card substrate 44, and here. Moreover, the head set section 48 for connecting the antenna section 46 which constitutes the transceiver section 42, LED47 turned on at the time of transmission and reception and headphone, a microphone, etc. is formed in the other end top face of the card substrate 44.

[0039] And the top face and inferior surface of tongue of the card substrate 44 are covered except for the other end with the metal coverings 50a and 50b of a pair by which fitting was carried out to the frame 43.

[0040] Moreover, it had the cap 51 which consists of synthetic resin, fitting of this cap 51 was carried out to the other end of the body 40 of a card, and the transceiver section 42 has covered the other end of the card substrate 44 and the antenna section 46 mounted in this other end top face, LED47, and the head set section 48.

[0041] In above-mentioned BT-PC card 20, the front end in which the connector 45 is formed turns into an insertion side edge to a card slot 26. And 1st guide slot 52a which carried out opening is formed in the top face of the body 40 of a card, a side face, and a front end side, and 2nd guide slot 52b which carried out opening only to the side face and front end side of the body 40 of a card is formed in the side-attachment-wall front end of another side of a frame 43 at one side-attachment-wall front end of a frame 43. In case these 1st and 2nd guide slots 52a and 52b equip a card slot 26 with BT-PC card 20, they regulate the sense of the front flesh side of BT-PC card 20.

[0042] BT-PC card 20 with which a personal computer 100 is equipped is also the same configuration, and it is equipped through the card slot 118 prepared in the lateral portion of a personal computer 100 as shown in drawing 1 .

[0043] The data communication which followed the radio specification of Bluetooth between the access point 10 and the personal computer 100 becomes possible by equipping an access point 10 and a personal computer 100 with BT-PC card 20 of such a configuration, respectively.

[0044] By the way, when a personal computer 100 accesses an access point 10, in the situation that an access point 10 and a personal computer 100 are connected for the first time, a personal computer 100 needs to input the PIN code of an access point 10. If an access point 10 has the right PIN code inputted from the personal computer 100, it will establish a link and will permit connection. When an access point 10 creates a link key based on ID of a personal computer 100, the own PIN code, etc. and there is a connection request from a personal computer 100 next time at this time, authentication by this link key will be performed.

[0045] The PIN code (authentication password) of an access point 10 is told only to the user to whom connection was permitted beforehand. However, when known by persons other than a user original with a certain means (using the software for example, only for code decode), it accesses unlawfully to an

access point 10 using the PIN code, and there is a problem which uses a public line 11 without notice.
[0046] Below, it explains preventing such unlawful access as main point.
[0047] Drawing 9 is the block diagram showing the radio structure of a system of this invention, and corresponds with the configuration of above-mentioned drawing 1 , a radio communications system is constituted from an access point 10 and a personal computer 100, and things are shown.
[0048] Here, with this operation gestalt, as shown in drawing 10 , slide switches 34a and 34b are formed in conspicuous locations, such as a rear face of an access point 10. These slide switches 34a and 34b are switches which can switch between 2 locations, and are for performing switch actuation in prohibition mode and authorization mode. Slide switch 34a forbids / permits the authentication actuation (registration actuation of a new device) in the PIN code, and slide switch 34b forbids / permits maintenance actuation (modification actuation of the PIN code or a link key) of security information.
[0049] The manager of an access point 10 performs fundamentally actuation of slide switches 34a and 34b, and slide switches 34a and 34b are usually set as the prohibition condition. And when registering a new device into an access point 10, a manager operates slide switch 34a and switches to an authorized state.
[0050] Thus, if slide switch 34a is switched to an authorized state and it considers as the prohibition condition usually when an original user newly connects, persons other than an original user can prevent inputting the PIN code of an access point 10 and accessing unlawfully in it.
[0051] Moreover, modification of the PIN code of an access point 10 and the maintenance of the security information memorized in a modem access point 10 called deletion of the link key of each device can be performed by inputting a command from the exterior (already registered device). It prevents accessing the security information in an access point 10 freely, and changing it by enabling activation of the maintenance of such security information, only when slide switch 34b is an authorized state.
[0052] In addition, it is possible to use the rotary switch 35 as independently indicated to be slide switches 34a and 34b to drawing 11 . This rotary switch 35 is made into what can switch between at least four locations. Both the authentication actuation (registration actuation of a new device) in the PIN code and maintenance actuation (modification actuation of the PIN code or a link key) of security information are forbidden in the 1st location. Both authentication actuation [according only maintenance actuation of security information to the PIN code in the 4th location only in authentication actuation] according to authorization in authorization and the 3rd location and the maintenance actuation of security information in the PIN code are permitted in the 2nd location.
[0053] The correspondence relation between slide switches 34a and 34b and a rotary switch 35 is shown in drawing 12 . SW1 in drawing shows slide switch 34a, SW2 shows slide switch 34b, OFF shows a prohibition condition and ON shows the authorized state. Moreover, 1-4 show the change location of a rotary switch 35.
[0054] The operating state of an access point 10 can be switched with slide switches 34a and 34b or a rotary switch 35 by giving the table showing the correspondence relation of such a slide switches 34a and 34b and a rotary switch 35 to an access point 10. However, as for a rotary switch 35, it is more desirable to operate it compared with slide switches 34a and 34b, and to switch the operating state of an access point 10 using slide switches 34a and 34b for a ****** reason. Below, it explains as what switches the operating state of an access point 10 using slide switches 34a and 34b.
[0055] Drawing 13 is the block diagram showing the circuitry of an access point 10 and BT-PC card 20.
[0056] As shown in drawing 13 , the access point 10 is equipped with CPU72 which controls actuation of the whole access point. LED24, the switch groups 34a, 34b, and 35, the connector 60 as a PC card interface, ROM73 and RAM74, nonvolatile memory 75, the RTC (Real TimeClock) circuit 76, etc. are connected to this CPU72. Moreover, the power source supplied from the AC adapter terminal 23 is supplied to CPU72 through the current supply section 77.
[0057] Furthermore, the access point 10 is equipped with the modem section 70 connected to a public line 11 through the modular cable 12 and a modular jack 32. This modem section 70 and the RS232C connector 22 are connected to CPU72 through the circuit changing switch 78. In addition, the modem

section 70 and a modular jack 30 function as the transceiver section.
[0058] ROM73 stores the communications protocol with radio and a public line 11 etc. RAM74 stores the driver software containing the program of operation, device driver, and radio protocol of an access point 10.
[0059] Moreover, the various storing sections 74a-74c for storing in this RAM74 the 1st control information of operation which controls authentication actuation of the PIN code here, the 2nd control information of operation which controls maintenance actuation of security information, and the criteria time information TM etc. are formed.
[0060] As nonvolatile memory 75, EEPROM is used, for example. While the link authentication error table T1 and T2 mentioned later are prepared, ID storing section 75a for holding own ID (it registering with BT-PC card 20), password storing section 75b for holding the own PIN code (password for authentication which the user created to arbitration), etc. are prepared in this nonvolatile memory 75.
[0061] The RTC circuit 76 is a circuit for clocking current time of day.
[0062] The modem section 70 changes into digital data the analog data which changed into the analog data the digital data inputted from BT-PC card 20, and transmitted to the public line 11 through the modular jack 32, and was inputted from the public line 11 through the modular jack 32, and transmits it to CPU72.
[0063] The RC232C connector 22 is formed in order to make serial connection of the external instrument and access point 10 of personal computer 100 grade through the RS232C cable which is not illustrated. For example, it is also possible to transmit the digital data which connected with the ISDN terminal adopter through the RC232C connector 22 and the RS232C cable in the access point 10, and was inputted from BT-PC card 20 as it is.
[0064] A circuit changing switch 78 switches connection with the public line 11 by the modem section 70 and the modular jack 32, and connection with other electronic equipment by the RS232C connector 22.
[0065] On the other hand, BT-PC card 20 with which this access point 10 is equipped is equipped with the antenna section 46, the RF section 80, the baseband section 81, memory 82, the Xtal oscillation section 83, the head set section 48, the AD/DA transducer 84, and LED47 as a wireless module of BT specification.
[0066] Transmission and reception of the data of BT-PC card 20 and an access point 10 are performed through a connector 45. The antenna section 46 performs transmission of the electric wave for performing radio, and reception, and the frequency band to be used has become 2.4-2.5GHz of BT specification. The RF section 80 performs signal processing which can perform a communication link on the frequency of the predetermined wireless electric wave to be used.
[0067] Moreover, the baseband section 81 carries out digital processing of the data inputted through the antenna section 46 and the RF section 80, and they are changed into the data which can be processed in an access point 10, it stores them in memory 82, and data are delivered and received between access points. In addition, ID shall be beforehand memorized by memory 82 here. ID which is not illustrated and which rewrote and was beforehand assigned to improper memory by BT-PC card 20 is memorized in fact, and ID of this BT-PC card 20 is written in nonvolatile memory 75 as identification information of a device proper at the time of BT-PC card 20 wearing.
[0068] LED47 is turned on at the time of transmission and reception of data. The Xtal oscillation section 83 supplies the criteria wave used in the RF section 80. The head set section 48 connects the head set which has headphone and a microphone, and outputs and inputs a sound signal. Moreover, the AD/DA transducer 84 changes into analog data the digital sound signal inputted through the baseband section 81 from an access point 10, and outputs it to the head set section 48 while it changes into digital data the sound signal of an analog inputted from the head set section 48.
[0069] drawing 14 comes out. The block diagram showing the circuitry of the personal computer 100 connected to an access point 10 as an external instrument, and BT-PC card 20.
[0070] It has the body 114 with which the keyboard 112 was formed as shown in a personal computer 100 at drawing 1 , and the liquid crystal display panel 116 prepared in this body 114 free [closing

motion]. A card slot 118 is formed in a body 114, and this card slot 118 is equipped with BT-PC card 20 free [desorption]. The configuration of a card slot 118 is almost the same as that of the card slot 26 of the access point 10 mentioned above. Moreover, BT-PC card 20 is as common as an access point 10, and since the internal configuration is the same as that of drawing 13 , it omits the explanation here.
[0071] Moreover, the personal computer 100 is equipped with CPU122 which controls the interface connector 120 of PCMCIA specification which transmits and receives data, and actuation of the whole personal computer between BT-PC cards 20. USB124, ROM126, RAM128, etc. are connected to CPU122.
[0072] USB124 is used in case serial connection is made through an access point 10 and the RS232C connector 22. Data, such as a program, are memorized by ROM126. Various kinds of data required for processing actuation of CPU122 are memorized by RAM128. Moreover, the PIN code (authentication password which the user created to arbitration) set as the personal computer 100, and the various data storage sections for setting which stored ID read from BT-PC card 20 are prepared in this RAM128.
[0073] Next, the configuration of the link authentication error table T1 and T2 which the access point 10 has managed is explained.
[0074] Drawing 15 is drawing showing the configuration of the link table T1.
[0075] ID (address) of a proper, the link key created based on the ID etc., the last connection time of day, and a data existence flag are registered into the link table T1 by each device.
[0076] As mentioned above, in an access point 10, when there is a connection request from a new device (device which is not registered into the link table T1), authentication in the PIN code is performed, in Authentication O.K., a link key is created based on ID of the device etc., and the link key is registered into the link table T1 with ID. Moreover, the connection time of day at this time is acquired from the RTC circuit 76, and it registers with the link table T1. The above-mentioned connection time of day is updated each time at the time of device connection. In addition, a data existence flag shows whether data are registered into the record column concerned.
[0077] Drawing 16 is drawing showing the configuration of the authentication error table T2.
[0078] As for the authentication error table T2, ID (address) of a proper, the authentication number of errors, the last connection time of day, and a data existence flag are registered into each device.
[0079] To the device judged on the occasion of the authentication in the PIN code to be an authentication error, an access point 10 matches ID and the authentication number of errors of the device, and registers them into the authentication error table T2. The initial value of the authentication number of errors is "1", and whenever a device is judged to be an authentication error, it is updated. Moreover, the connection time of day at this time is acquired from the RTC circuit 76, and it registers with the authentication error table T2. The above-mentioned connection time of day is updated each time at the time of device connection. In addition, a data existence flag shows whether data are registered into the record column concerned.
[0080] The number of registration of the link authentication error table T1 and T2 is decided according to the capacity of nonvolatile memory 75, and the maximum registration number of cases of the authentication error table T2 of the maximum registration number of cases of the link table T1 is M affairs in the example of N affair and drawing 16 in the example of drawing 15 .
[0081] Next, actuation of this system is explained.
[0082] Here, it divides into switch processing of the operating state by the (a) switch, connection processing with the (b) external instrument, maintenance processing of (c) security information, and authentication error processing at the time of (d) connection as processing for preventing unlawful access to an access point 10, and explains.
[0083] (a) As the operating state by the switch carried out switch processing ****, the slide switches 34a and 34b for switching the operating state of an access point 10 are formed in the rear face of an access point 10. Slide switch 34a makes authentication actuation in the PIN code a prohibition condition or an authorized state, and slide switch 34b makes maintenance actuation of security information a prohibition condition or an authorized state.
[0084] Here, change processing of the operating state by slide switch 34a is explained.

[0085] Drawing 17 is a flow chart which shows change processing of the operating state by slide switch 34a prepared in the access point 10. In addition, drawing 17 shows processing of the program which CPU72 of an access point 10 performs. Moreover, the inside SW1 of drawing is slide switch 34a.
[0086] In the access point 10, the condition of slide switch 34a is always supervised. If it detects that slide switch 34a was switched to the authorized state from the prohibition condition (Yes of step A11), first, an access point 10 will acquire current time from the RTC circuit 76 shown in drawing 13 , and will set it to criteria time-of-day storing section 74c in RAM74 by making this time of day into the criteria time information TM (step A12). And the 1st control information of operation which considers authentication actuation of the PIN code as authorization is set to 1st of operation control information storing section 74a in RAM74 (step A13).
[0087] On the other hand, an access point 10 will set to 1st of operation control information storing section 74a in RAM74 the 1st control information of operation which considers authentication actuation of the PIN code as prohibition, if it detects that slide switch 34a was switched to the prohibition condition from the authorized state (Yes of step A14) (step A15).
[0088] Moreover, if the difference of the criteria time information TM and current time which were set at the time of the switch becomes beyond predetermined time after slide switch 34a is switched to an authorized state from a prohibition condition After slide switch 34a is switched to an authorized state, when predetermined time progress is carried out (Yes of step A16), that is, an access point 10 Regardless of the condition of slide switch 34a, the 1st control information of operation which considers authentication actuation of the PIN code as prohibition is set to 1st of operation control information storing section 74a (step A17).
[0089] The same is said of slide switch 34b.
[0090] That is, if slide switch 34b is switched to an authorized state from a prohibition condition, while the time of day at that time will be set to criteria time-of-day storing section 74c in RAM74 as criteria time information TM, the 2nd control information of operation which considers maintenance actuation of security information as authorization is set to 2nd of operation control information storing section 74b in RAM74. On the other hand, if slide switch 34b is switched to a prohibition condition from an authorized state, the 2nd control information of operation which considers maintenance actuation of security information as prohibition will be set to 2nd of operation control information storing section 74b in RAM74.
[0091] Furthermore, after slide switch 34b was switched to the authorized state from the prohibition condition, If the difference of the criteria time information TM (it considers as a thing other than what manages slide switch 34a) and current time which were set at the time of the switch becomes beyond predetermined time That is, if predetermined time progress is carried out after slide switch 34b is switched to an authorized state Regardless of the condition of slide switch 34b, the 2nd control information of operation which considers maintenance actuation of security information as prohibition is set to 2nd of operation control information storing section 74b in RAM74.
[0092] In addition, although about 10 minutes is appropriate to the above-mentioned predetermined time, you may decide on the time amount beforehand, and the manager of an access point 10 may enable it to set it as arbitration.
[0093] (b) Explain connection processing with an external instrument, next connection processing with an external instrument.
[0094] Drawing 18 is a flow chart which shows the actuation of connection processing with an external instrument in an access point 10. In addition, drawing 18 shows processing of the program which CPU72 of an access point 10 performs.
[0095] For example, if a connection request is sent by radio to an access point 10 from the personal computer 100 which is an external instrument, an access point 10 will confirm first whether the authentication actuation in the PIN code is permitted based on the 1st control information of operation stored in 1st of operation control information storing section 74a in RAM74 (step B11).
[0096] As for the 1st control information of operation, authorization is shown when predetermined time progress has not been carried out, after slide switch 34a is switched to the authorized state and slide

switch 34a is switched to an authorized state, as mentioned above. Moreover, after slide switch 34a is switched to the prohibition condition or slide switch 34a is switched to an authorized state, when predetermined time progress is being carried out, the 1st control information of operation shows prohibition.

[0097] If the authentication actuation in the PIN code is permitted (Yes of step B12), the personal computer 100 of the connection-request point will check an access point 10 by the existence [as opposed to a personal computer 100 for whether it is the first connection] of a link key (step B13). That is, ID and the link key of the device connected to the access point 10 until now are registered into the link table T1 which an access point 10 has. If there is no link key to a personal computer 100 in this link table T1 and in other words ID of a personal computer 100 is not registered into the link table T1, a personal computer 100 is judged to be the first connection.

[0098] Here, in the situation that an access point 10 and a personal computer 100 are connected for the first time (Yes of step B13), it is necessary to input the PIN code of an access point 10 from a personal computer 100.

[0099] If the PIN code is inputted from a personal computer 100, an access point 10 will perform authentication in this PIN code (step B14). When the above-mentioned PIN code is in agreement with the PIN code of the self stored in password storing section 75b within the right case 75, i.e., nonvolatile memory, it judges with authentication being possible (Yes of step B15).

[0100] Here, the authentication actuation in the PIN code is concretely explained with reference to drawing 22 .

[0101] Now, the case where Device A connects with Device B is assumed. With this operation gestalt, a personal computer 100 and Device B are equivalent to an access point 10 for Device A. Moreover, the password in drawing is the PIN code of an access point 10.

[0102] As shown in drawing 22 , Device A transmits a connection demand (connection request) first (step S1). If the connection demand from Device A is received, it analyzes these received data, and Device B will transmit the message of connection establishment to Device A, when satisfactory (step S2), and a connection will establish it between device A-B after an appropriate time (step S3). In addition, the connection in this case shall mean the connection of a communicative lower order layer, shall mean the situation "the temporary network address was given", and does not necessarily mean service of high order application.

[0103] After the above-mentioned connection is established, authentication procedure with a password is performed. That is, if the above-mentioned connection is established, Device B will output an authentication demand to Device A, and the input of a password will be urged to it (step S4). Thereby, the user of Device A enters the password of Device B, and transmits it (step S5).

[0104] The device B which received the above-mentioned password collates the password of a self-opportunity, and the received password. If the collating result is wrong, the message of the purport from which a password is different will be returned to Device A, but authentication will be completed if there is no problem in a collating result (step S6).

[0105] As a result of returning to drawing 18 and performing authentication actuation in the above PIN codes, when judged with authentication being possible, (Yes of step B15) and an access point 10 establish a link (step B16), and create the link key to a personal computer 100 (step B17). In detail, ID of a personal computer 100 is acquired, the random number which generates the PIN code of the ID and self etc. in an access point 10 side is multiplied, and a link key with difficult decode is created. And an access point 10 registers into the link table T1 the link key by which creation was carried out [above-mentioned] with ID of a personal computer 100 (step B18). While acquiring current time of day from the RTC circuit 76 and registering with the link table T1 by making time of day at that time into the last connection time of day in that case, the data existence flag is set to "**."

[0106] Here, if there is no opening in the link table T1 in case the data of a new device are registered into the link table T1 (all data existence flags are the conditions of **), the data of the oldest device of the last connection time of day shall be deleted from the link table T1, and the data of a new device shall be registered [then,]. Thus, by registering the link key of the device newly connected instead of the link

key of the low device of possibility of connecting, priority can be given to a new connection partner in the registration number of cases (the example of drawing 15 N affair) of the link table T1 prepared in nonvolatile memory 75, the PIN code can be managed efficiently, and user-friendliness can be raised.
[0107] In addition, it is possible to store the count of access to this device of each device in the link table T1, for example, and to delete the data of fewest devices of the count of access.
[0108] Moreover, it is possible to store the registration time of day to the link table T1 of each device in the link table T1, and to delete the data of the oldest device of the registration time of day.
[0109] If the authentication in the PIN code is O.K., connection between an access point 10 and a personal computer 100 will be established, and the data communication by wireless will become mutually possible (step B19). Moreover, when the authentication in the PIN code is NG, (No of step B15) and an access point 10 refuse connection with the personal computer 100 which is the connection-request point at that time.
[0110] On the other hand, when the authentication actuation in the PIN code is forbidden (No of step B12), or when a personal computer 100 may be connected to an access point 10 before, (No of step B13) and an access point 10 perform authentication by the link key (step B20). In this case, if the personal computer 100 of the connection-request point may be connected to an access point 10 before, since the link key to a personal computer 100 is registered into the link table T1, it can attest using that link key. If it is Authentication O.K. (Yes of step B21), an access point 10 will establish connection with a personal computer 100 (step B19). Moreover, when the authentication in the PIN code is NG, (No of step B21) and an access point 10 refuse connection with the personal computer 100 which is the connection-request point at that time.
[0111] Thus, only when the authentication actuation in the PIN code is permitted, a new device can try access to an access point 10. Therefore, since it cannot access to an access point 10 usually even if persons other than an original user receive the PIN code of an access point 10 with a certain means if the authentication actuation in the PIN code is forbidden by actuation of slide switch 34a, a public line 11 can prevent the malfeasance of using it without notice.
[0112] Moreover, since the authentication actuation in the PIN code will be automatically forbidden regardless of the condition of slide switch 34a if predetermined time progress is carried out even if the manager of an access point 10 forgets to switch slide switch 34a to a prohibition condition, the security of an access point 10 can be strengthened.
[0113] (c) Explain maintenance processing of security information, next maintenance processing of security information.
[0114] Drawing 19 is a flow chart which shows actuation of maintenance processing of the security information in an access point 10. In addition, drawing 19 shows processing of the program which CPU72 of an access point 10 performs.
[0115] Where connection with the personal computer 100 which is an external instrument is established now, the maintenance command of security information should be transmitted from wireless from (step C11) and a personal computer 100. The maintenance command of security information has read-out of the PIN code, read-out of rewriting and the link table T1, deletion, etc.
[0116] An access point 10 will confirm first whether maintenance actuation of security information is permitted based on the 2nd control information of operation stored in 2nd of operation control information storing section 74b in RAM74, if the above-mentioned maintenance command is received (step C12).
[0117] As for the 2nd control information of operation, authorization is shown when predetermined time progress has not been carried out, after slide switch 34b is switched to the authorized state and slide switch 34b is switched to an authorized state, as mentioned above. Moreover, after slide switch 34b is switched to the prohibition condition or slide switch 34b is switched to an authorized state, when predetermined time progress is being carried out, the 2nd actuation control information shows prohibition.
[0118] If maintenance actuation of security information is forbidden (No of step C13), an access point 10 will refuse the above-mentioned maintenance command (step C14). Thereby, security information is

unmaintainable no matter it may be what external instrument.
[0119] On the other hand, if maintenance actuation of security information is permitted (Yes of step C13), as for an access point 10, the above-mentioned maintenance command will be executed (step C15). In that case, when rewriting of the PIN code is performed, as for (Yes of step C16), and an access point 10, all the data of the link table T1 are deleted (step C17).
[0120] Thus, only when maintenance actuation of security information is permitted, a command can be sent from an external instrument and rewriting of the PIN code etc. can be performed. Therefore, if maintenance actuation of security information is usually forbidden by actuation of slide switch 34b, since security information cannot be accessed freely, the security of an access point 10 is securable.
[0121] Moreover, since maintenance actuation of security information will be automatically forbidden regardless of the condition of slide switch 34b if predetermined time progress is carried out even if the manager of an access point 10 forgets to switch slide switch 34b to a prohibition condition, the security of an access point 10 is securable.
[0122] Furthermore, security can be further strengthened with clearing all the data of the link table T1 in consideration of the possibility of an alteration of the data by the unlawful access person, when the PIN code is changed. When the link table T1 is cleared, it will ask for the input of the PIN code again from all external instruments. In this case, the user who does not know the PIN code newly set up in the access point 10 can connect with an access point 10.
[0123] (d) Explain authentication error processing at the time of connection, next authentication error processing at the time of connection.
[0124] Drawing 20 and drawing 21 are flow charts which show actuation of authentication error processing at the time of the connection in an access point 10. In addition, drawing 20 and drawing 21 show processing of the program which CPU72 of an access point 10 performs.
[0125] Now, ID of the personal computer 100 which is an external instrument shall not be registered into the link table T1. If there is a connection request from this personal computer 100 (step D11), refer to the authentication error table T2 for an access point 10 (step D12). As shown in drawing 16 , ID of the device which became an authentication error before etc. is registered into the authentication error table T2.
[0126] When ID of a personal computer 100 is not registered into this authentication error table T2, it usually passes along (No of step D13), and an access point 10, and authentication in the PIN code is performed (step D14). And if it is Authentication O.K. (Yes of step D15) (i.e., if the PIN code which the personal computer 100 inputted is in agreement with the PIN code of an access point 10), an access point 10 will permit connection of a personal computer 100 (step D16).
[0127] On the other hand, when it is an authentication error (i.e., when the PIN code which the personal computer 100 inputted is not in agreement with the PIN code of an access point 10), as for (No of step D15), and an access point 10, connection of a personal computer 100 is refused (step D17). While an access point 10 acquires ID of a personal computer 100 and registering the ID into the authentication error table T2 in that case, the number of errors corresponding to Above ID is made into initial value "1", further, current time of day is acquired from the RTC circuit 76, and the time of day is registered as last connection time of day (step D18).
[0128] Moreover, suppose that ID of the personal computer 100 of the connection-request point was registered into the link table T1 in the above-mentioned step D13. That is, suppose that it was refused noting that the PIN code inputted from the personal computer 100 before was not right.
[0129] In such a case, it sets and an access point 10 first confirms whether the number of errors corresponding to ID of the personal computer 100 in the authentication error table T2 is over the count of predetermined (step D19). Consequently, if the number of errors is less than a count of predetermined (No of step D19), it will usually pass along an access point 10, and authentication in the PIN code will be performed (step D20). And if it is Authentication O.K. (Yes of step D21) (i.e., if the PIN code which the personal computer 100 inputted is in agreement with the PIN code of an access point 10), an access point 10 will permit connection of a personal computer 100 (step D22). At this time, the data about a personal computer 100 are deleted from the authentication error table T2 (step D23).

[0130] On the other hand, when the number of errors is over the count of predetermined, it judges that (No of step D19) and a personal computer 100 are unlawful access persons, and connection of a personal computer 100 is refused (step D24). While updating the number of errors of the personal computer 100 concerned in the authentication error table T2 in that case, current time of day is acquired from the RTC circuit 76, and it updates as last connection time of day (step D25). Moreover, also when it becomes an authentication error in the above-mentioned step D21, it is at this appearance, and the data about the personal computer 100 concerned in the authentication error table T2 are updated with refusal of connection (steps D24 and D25).
[0131] Thus, the count at the time of becoming an authentication error is counted at the time of the authentication in the PIN code, and the same device can prevent inputting the PIN code repeatedly and accessing an access point 10 unjustly, and can strengthen the security of an access point 10 with refusing connection of the device concerned completely, when the authentication number of errors of the same device exceeds the count of predetermined.
[0132] In addition, although about 5 times is appropriate to the above-mentioned count of predetermined, the count may be decided beforehand and the manager of an access point 10 may enable it to set it as arbitration.
[0133] Moreover, if there is no opening in the authentication error table T2 in case the data of a new device are registered into the authentication error table T2 (all data existence flags are the conditions of **), the data of the oldest device of the last connection time of day will be deleted from the authentication error table T2, and the data of a new device will be registered there. Thus, by deleting old data, priority can be given to a new connection partner in the registration number of cases (the example of drawing 16 M affairs) of the authentication error table T2 prepared in nonvolatile memory 75, the authentication number of errors can be managed efficiently, and user-friendliness can be raised.
[0134] As mentioned above, unjust access from the outside can be prevented and security can be strengthened with forbidding the authentication actuation and the maintenance actuation of security information in the PIN code by actuation of the switch formed in the access point 10. Furthermore, regardless of the condition of a switch, by switching automatically the authentication actuation and the maintenance actuation of security information in the PIN code to a prohibition condition after predetermined time progress, even if a manager forgets switch actuation, security is securable.
[0135] Moreover, when there is an input of the inaccurate PIN code repeatedly from the same device, those who do not know the right PIN code can prevent trying unlawful access by refusing connection of the device completely henceforth.
[0136] moreover, in registering a link key with a new connection partner after reaching the maximum number which can memorize the registered number-of-cases number of the link keys to the link table T1 prepared in nonvolatile memory 75 By deleting the link key already memorized according to fixed regulations (what has old connection time of day, what has low access frequency), and registering a new link key into the field Priority can be given to a new connection partner, PIN code input at the time of connection of the henceforth can be made unnecessary, and user-friendliness can be raised.
[0137] Moreover, security can be strengthened with deleting all the link keys of each device registered into the link table T1, and having required the input of the new PIN code at the time of connection when the PIN code in an access point 10 is changed.
[0138] By the way, ID of BT module is registered into BT-PC card 20 with which each device is equipped, and when an access point 10 is equipped with BT-PC card 20, CPU72 shown in drawing 15 stores in ID storing section 75a of the nonvolatile memory 75 in an access point 10 ID registered into BT-PC card 20 as information on a device proper.
[0139] Here, when CPU72 detects having been exchanged in BT-PC card 20 through the connector 60 as a PC card interface, all the data of the link table T1 are deleted and each device is connected, processing in which a link key is newly re-created is performed.
[0140] This is because it may be equipped with BT module other than BT module with which the access point 10 was first equipped by a user's mistake, when BT module (ID is memorized) consists of exchangeable units, such as a PC card. That is, since a link key is what is created based on ID etc., it it

leaves the link key created by ID before BT module exchange as it is, conflict with the link key created by ID after BT module exchange arises, and connection with an external instrument becomes impossible [a key]. In order to cancel such fault, when are exchanged in BT module, and all the data registered into the current link table T1 are deleted and each device is connected, processing in which a link key is newly re-created is performed.

[0141] In addition, although this invention is effective especially when accessing unlawfully by wireless from the external instrument in the location distant from the access point 10, it does not necessarily need to be wireless as an access means to an access point 10. That is, even if it is the system to which the access point 10 shown, for example in drawing 1 and a personal computer 100 are connected through a telecommunication cable, unlawful access can be prevented by applying the same technique with the above-mentioned operation gestalt.

[0142] Moreover, although the access point 10 equipped with the connect function of a public line 11 was made into the example and the above-mentioned operation gestalt explained it, if it is the device equipped with the communication facility for making connection with other devices by wireless etc., the technique of this invention is applicable to all those devices.

[0143] Moreover, it is not necessary to consist of exchangeable units, such as a PC card, as a radio module used for each device, and may be built in the device.

[0144] Moreover, as a radio method, you may be not only Bluetooth but other methods.

[0145] in short, this invention is not limited to the above-mentioned operation gestalt, and in the range which does not deviate from the summary, many things are boiled and it can be deformed at an execution phase Furthermore, invention of various phases is included in the above-mentioned operation gestalt, and various invention may be extracted by the proper combination in two or more requirements for a configuration indicated. For example, even if some requirements for a configuration are deleted from all the requirements for a configuration shown with an operation gestalt, the effectiveness stated by "Object of the Invention" is solvable, and when the effectiveness stated in the column of a "effect of the invention" is acquired, the configuration from which this requirement for a configuration was deleted may be extracted as invention.

[0146] Moreover, as a program which a computer can be made to execute, it writes in record media, such as magnetic disks (a floppy (trademark) disk, hard disk, etc.), optical disks (CD-ROM, DVD, etc.), and semiconductor memory, and it applies to various equipments, or it transmits by communication media, and the technique indicated in the operation gestalt mentioned above can also be applied to various equipments. The computer which realizes this equipment performs processing mentioned above by reading the program recorded on the record medium and controlling actuation by this program.

[0147]

[Effect of the Invention] As a full account was given above, according to this invention, authentication by specific identification code is forbidden or permitted according to the condition of a switch. Therefore, though the above-mentioned specific identification code can be known unjustly, unless setting actuation of the above-mentioned switch is carried out directly, a link with this device cannot be stretched. Furthermore, since authentication by the above-mentioned specific identification code is forbidden automatically, after predetermined time progress can secure security, though a manager has forgotten to return a switch to a prohibition condition.

[0148] Moreover, the modification actuation to the various management information for connecting among other devices is forbidden or permitted according to the condition of a switch. Therefore, even if the inaccurate user of other devices is able to connect with this device, unless setting actuation of the above-mentioned switch is carried out directly, various management information cannot be changed freely. Furthermore, since modification of the various above-mentioned management information is forbidden automatically, after predetermined time progress can secure security, though a manager has forgotten to return a switch to a prohibition condition.

[0149] Moreover, since the connection request from the device which became an authentication error exceeding the count of predetermined is refused, the attempt of the unjust connection from the same device can be prevented.

[0150] Moreover, in the condition that there is the registration number of cases of memory to the limit, since the low link information of the possibility of connection is deleted in it and the link information of a new device is registered, user-friendliness can be raised.
[0151] Moreover, since all the link informations in memory are deleted when specific identification code is changed, unlawful access from the user who does not know new identification code can be prevented.
[0152] Moreover, in electronic equipment equipped with the exchangeable radio unit, since all the link informations in memory are deleted when there is exchange of a radio unit, it can prevent that lose conflict with the link information created by the identification code of the radio unit before exchange, and the link information created by the identification code of the radio unit after exchange, and connection with other devices becomes impossible.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The perspective view showing the appearance configuration of the radio communications system concerning 1 operation gestalt of this invention.
[Drawing 2] The decomposition perspective view of an access point used for the above-mentioned radio communications system.
[Drawing 3] The perspective view showing the condition of having used the above-mentioned access point in every length.
[Drawing 4] The perspective view showing the tooth-back side of the above-mentioned access point.
[Drawing 5] The perspective view showing the condition of having used the above-mentioned access point by every side.
[Drawing 6] The perspective view showing the base side of the above-mentioned access point.
[Drawing 7] The perspective view of BT-PC card with which the above-mentioned access point is equipped.
[Drawing 8] The decomposition perspective view of the above-mentioned BT-PC card.
[Drawing 9] The block diagram showing the above-mentioned radio structure of a system.
[Drawing 10] Drawing showing the configuration of the slide switch formed in the above-mentioned access point.
[Drawing 11] Drawing showing the configuration of the rotary switch formed in the above-mentioned access point.
[Drawing 12] Drawing showing the correspondence relation between the above-mentioned slide switch and the above-mentioned rotary switch.
[Drawing 13] The block diagram showing the circuitry of the above-mentioned access point and BT-PC card.
[Drawing 14] The block diagram showing the circuitry of the personal computer connected to the above-mentioned access point as an external instrument, and BT-PC card.
[Drawing 15] Drawing showing the configuration of the link table prepared in the above-mentioned access point.
[Drawing 16] Drawing showing the configuration of the authentication error table prepared in the above-mentioned access point.
[Drawing 17] The flow chart which shows change processing of the operating state by the slide switch formed in the above-mentioned access point.
[Drawing 18] The flow chart which shows the actuation of connection processing with an external instrument in the above-mentioned access point.
[Drawing 19] The flow chart which shows actuation of maintenance processing of the security information in the above-mentioned access point.
[Drawing 20] The flow chart which shows actuation of authentication error processing at the time of the connection in the above-mentioned access point.
[Drawing 21] The flow chart which shows actuation of authentication error processing at the time of the

connection in the above-mentioned access point.
[Drawing 22] Drawing for explaining the authentication actuation in the PIN code.
[Description of Notations]
10 -- Access point
12 -- Modular cable
14 -- Body of a device
20 -- BT-PC card
34a, 34b -- Slide switch
35 -- Rotary switch
40 -- Body of a card
42 -- Transceiver section
46 -- Antenna section
45 60 -- Connector
70 -- Modem section
72 -- CPU
74 -- RAM
74a -- The 1st control information storing section of operation
74b -- The 2nd control information storing section of operation
74c -- Criteria time-of-day storing section
75 -- Nonvolatile memory
75 a--ID storing section
75b -- Password storing section
T1 -- Link table
T2 -- Authentication error table
76 -- RTC circuit
100 -- Personal computer
112 -- Keyboard
116 -- The LCD panel
120 -- Interface connector
122 -- CPU

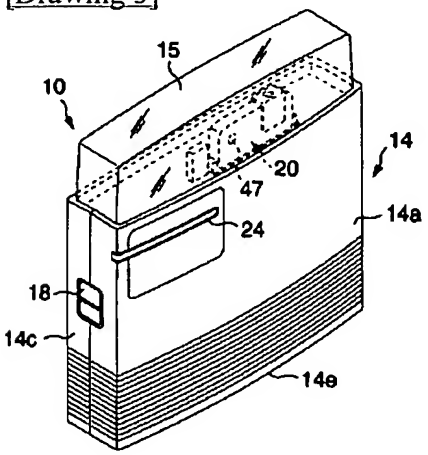
[Translation done.]

* NOTICES *

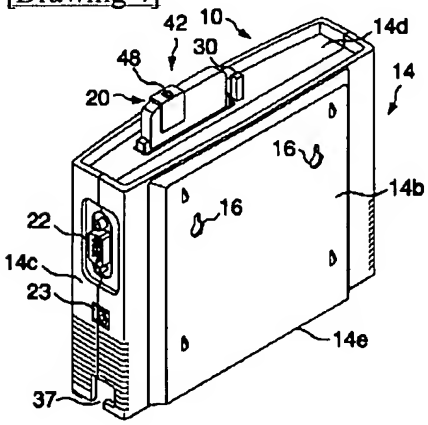
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

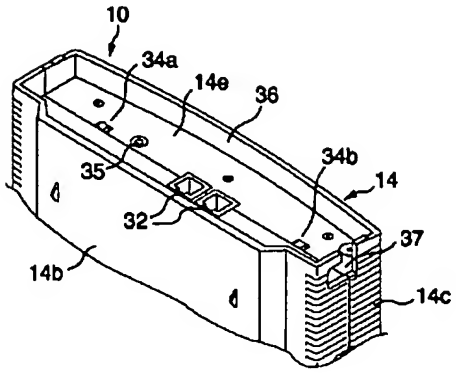
[Drawing 3]



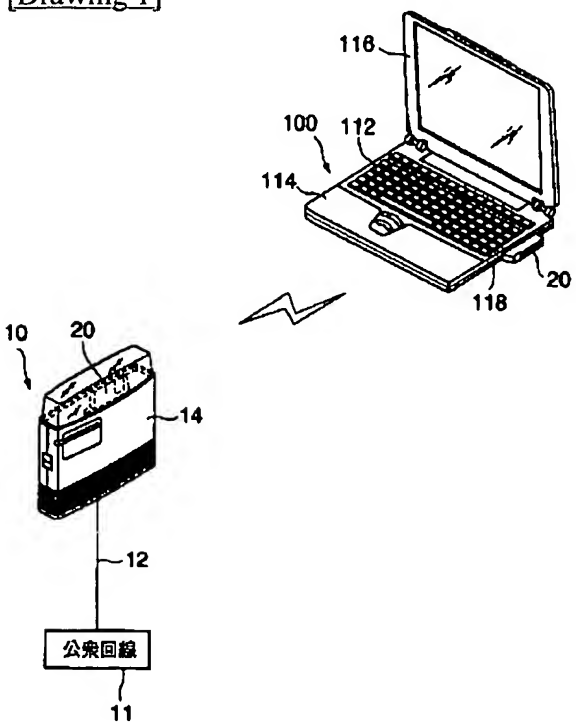
[Drawing 4]



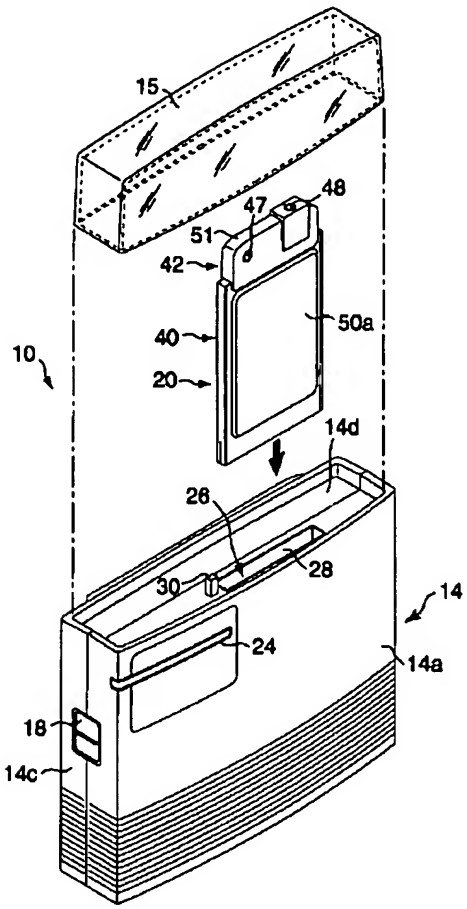
[Drawing 6]



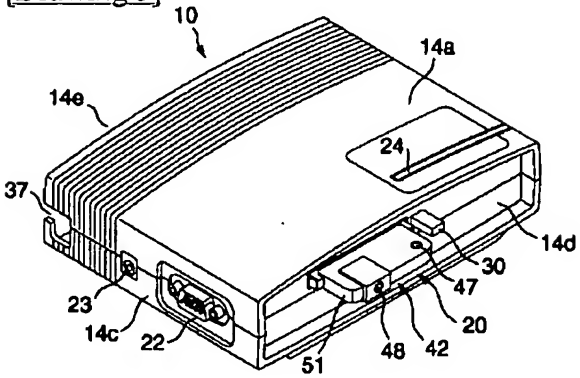
[Drawing 1]



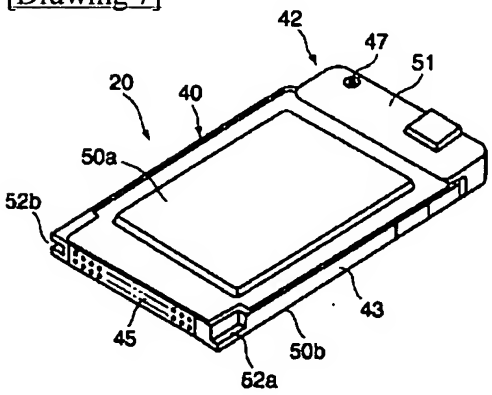
[Drawing 2]



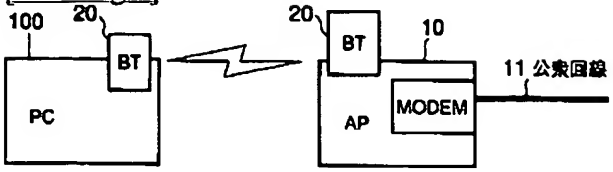
[Drawing 5]



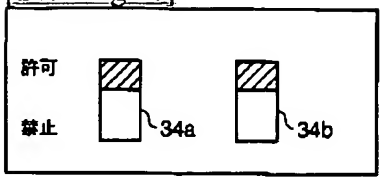
[Drawing 7]



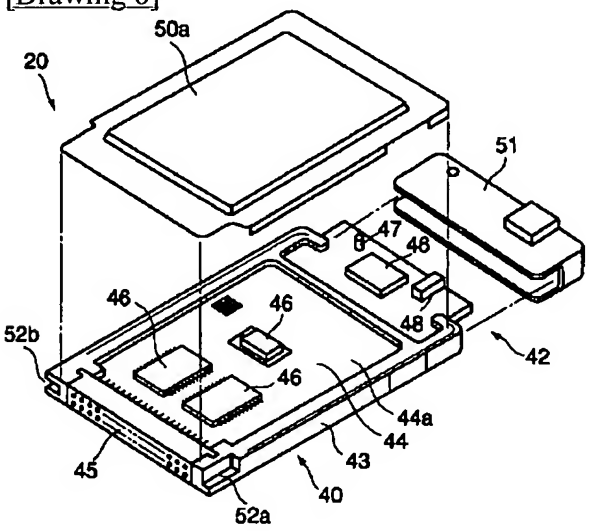
[Drawing 9]



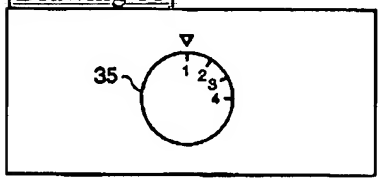
[Drawing 10]



[Drawing 8]



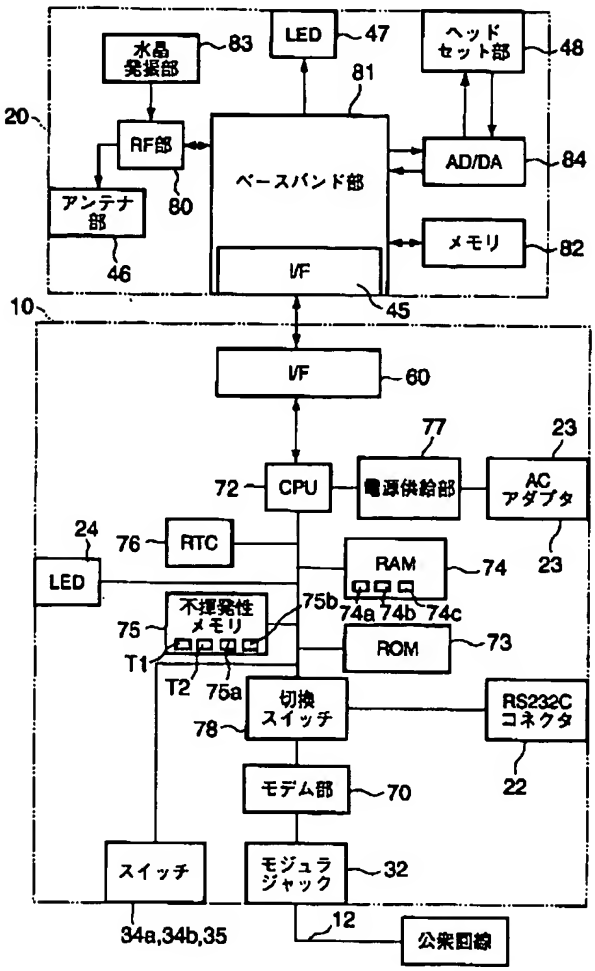
[Drawing 11]



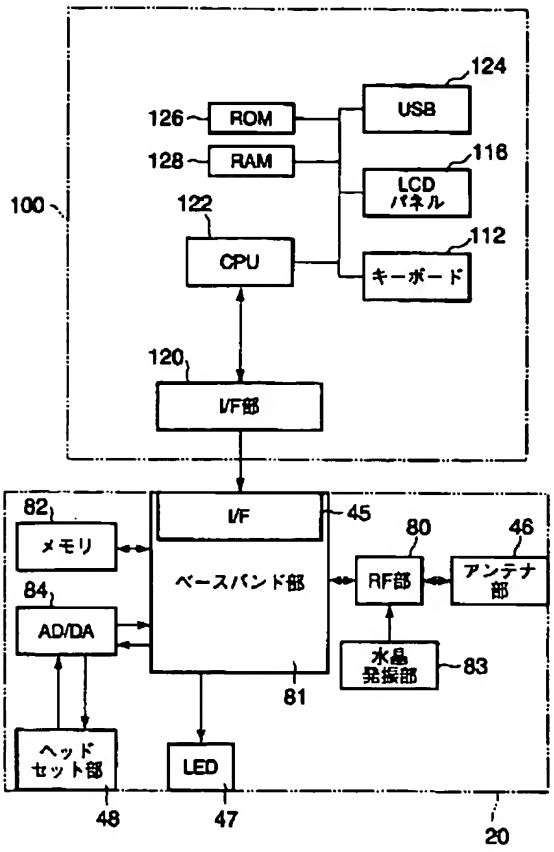
[Drawing 12]

SW1	SW2	ロータリースイッチ
OFF	OFF	1
ON	OFF	2
OFF	ON	3
ON	ON	4

[Drawing 13]


水晶発振部
83
LED
47
ヘッドセット部
48
81
20
RF部
80
ベースバンド部
AD/DA
84
アンテナ部
46
メモリ
82
I/F
45
10
I/F
60
77
23
72
CPU
電源供給部
ACアダプタ
24
76
RTC
RAM
74
23
LED
不揮発性メモリ
75b
74a
74b
74c
75
ROM
73
T1
T2
75a
切換スイッチ
RS232Cコネクタ
78
モデム部
70
22
スイッチ
モジュラジャック
32
12
34a,34b,35
公衆回線

[Drawing 14]



[Drawing 15]

T1 リンクテーブル

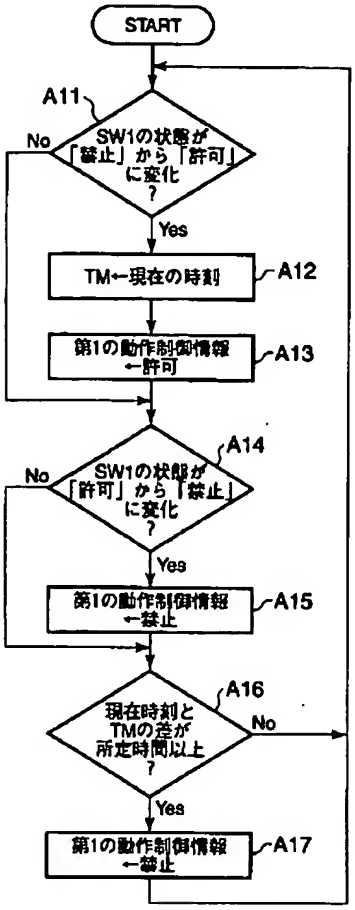
番号	ID (Hex)	リンクキー	最終接続時刻	データ有無フラグ
1	A36B35	XXXXXX	2000/07/20/12:00:10	有
2	4B3346	xxxxxx	2000/05/20/11:00:07	有
	⋮	⋮		
N-1	87647A	oooooo	2000/08/12/16:30:37	有
N	—	—		無

[Drawing 16]

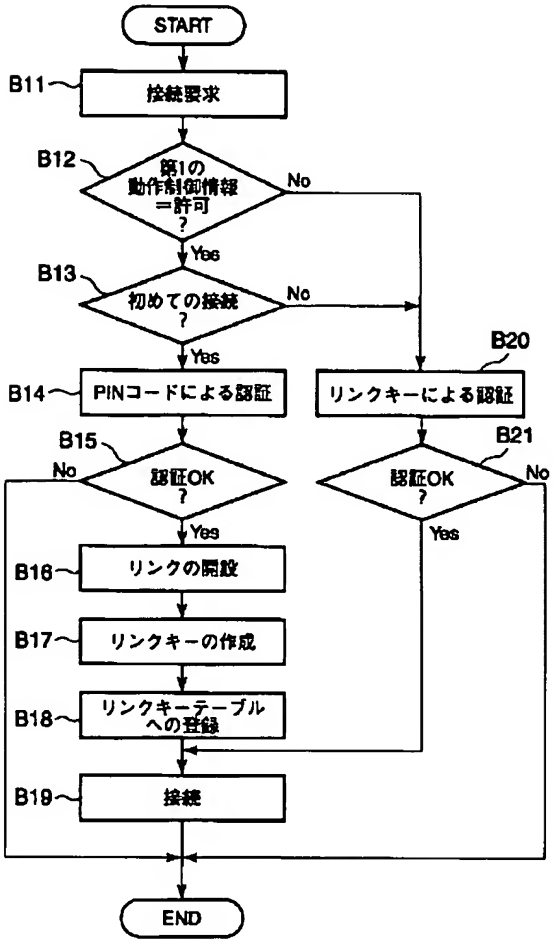
T2 認証エラーテーブル

番号	ID (Hex)	認証エラー回数	最終接続時刻	データ有無フラグ
1	A36B35	2	2000/07/20/12:00:10	有
2	4B3346	5	2000/05/20/11:00:07	有
	⋮	⋮		
M-1	87647A	1	2000/08/12/16:30:37	有
M	—	—		無

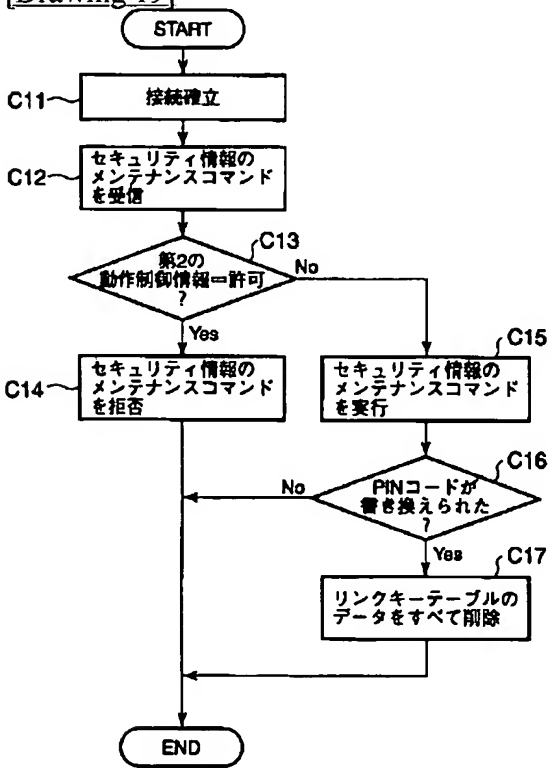
[Drawing 17]


START
A11
SW1の状態が「禁止」から「許可」に変化？
No
Yes
TM←現在の時刻
A12
第1の動作制御情報←許可
A13
A14
SW1の状態が「許可」から「禁止」に変化？
No
Yes
第1の動作制御情報←禁止
A15
A16
現在時刻とTMの差が所定時間以上？
No
Yes
第1の動作制御情報←禁止
A17

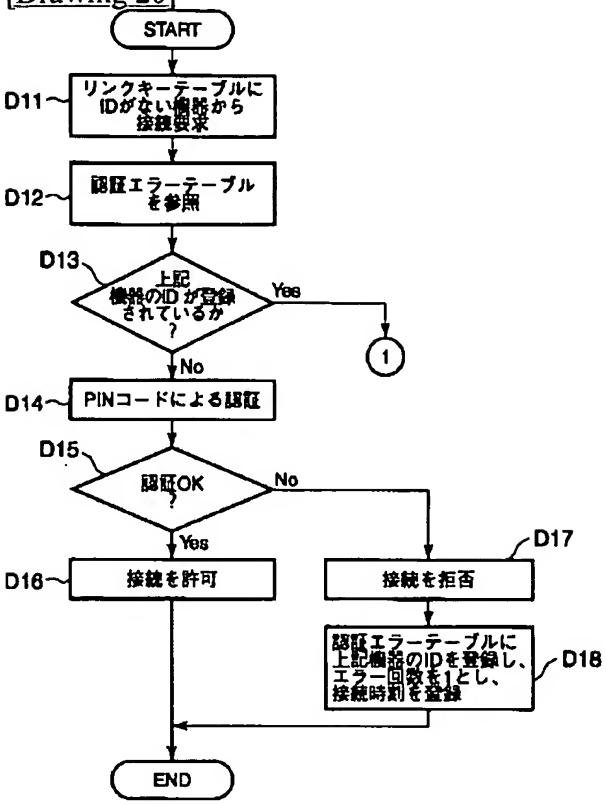
[Drawing 18]


START
B11
接続要求
B12
第1の動作制御情報=許可?
No
Yes
B13
初めての接続?
No
Yes
B20
B14
PINコードによる認証
リンクキーによる認証
B15
B21
No
認証OK?
認証OK?
No
Yes
Yes
B16
リンクの開設
B17
リンクキーの作成
B18
リンクキーテーブルへの登録
B19
接続
END

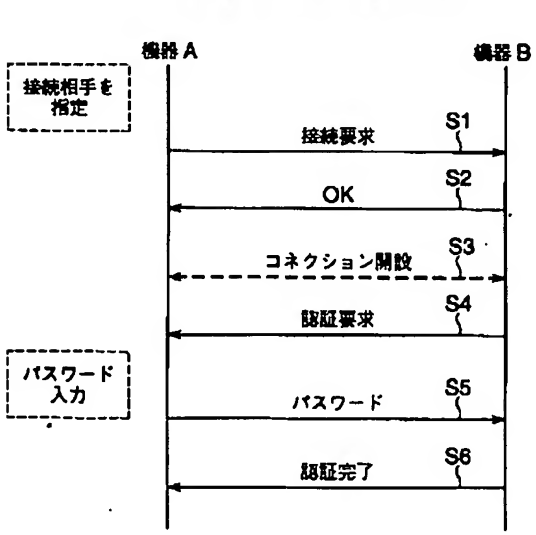
[Drawing 19]


START
C11
接続確立
C12
セキュリティ情報のメンテナンスコマンドを受信
C13
第2の動作制御情報=許可?
No
Yes
C15
C14
セキュリティ情報のメンテナンスコマンドを拒否
セキュリティ情報のメンテナンスコマンドを実行
C16
No
PINコードが書き換えられた?
Yes
C17
リンクキーテーブルのデータをすべて削除
END

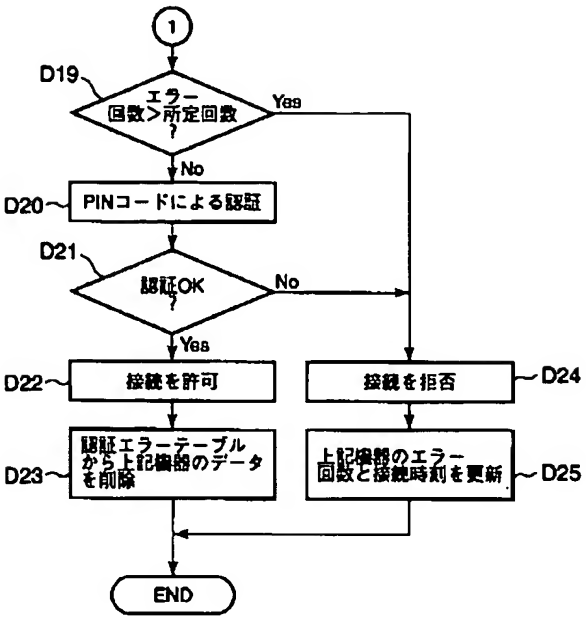
[Drawing 20]



[Drawing 22]



[Drawing 21]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－77999
（P2002－77999A）
(43)公開日　平成14年３月15日(2002.3.15)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０３３
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ	５Ｋ０６７

審査請求　有　　請求項の数19　ＯＬ　（全 20 頁）

(21)出願番号　特願2000－255840(P2000－255840)

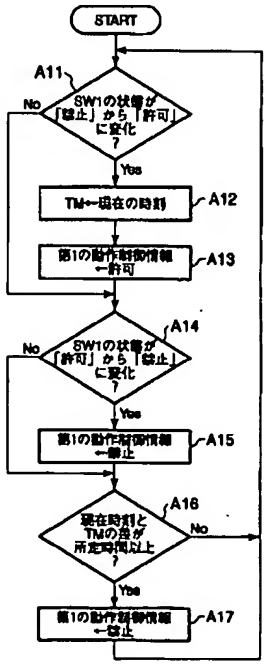
(22)出願日　平成12年８月25日(2000.8.25)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　伊藤　隆文
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5K033 AA08 CB01 DA17 DB12
5K067 AA32 AA34 CC10 DD17 DD27
DD30 EE02 EE25 EE35 FF05
HH22 HH23 HH24 HH36 KK15

(54)【発明の名称】　電子機器及び接続制御方法

(57)【要約】
【課題】他の機器からの不正アクセスを防止してセキュリティを確保する。
【解決手段】機器本体にスイッチを設け、このスイッチが許可状態に切り換えられた場合には、特定の識別コード（ＰＩＮコード）による認証を許可し（ステップＡ１１～Ａ１３）、スイッチが禁止状態に切り換えられた場合には上記特定の識別コードによる認証を禁止する（ステップＡ１４、Ａ１５）。これにより、普段はスイッチを禁止状態にしておくことで、不正アクセス者が特定の識別コードを用いてアクセスすることを防ぐことができる。また、スイッチが許可状態にあるときから所定時間経過した場合に、上記特定の識別コードによる認証を禁止する（ステップＡ１６、Ａ１７）。これにより、スイッチを許可状態にした後で禁止状態に戻し忘れたとしても、不正アクセスを防いで機器のセキュリティを確保できる。



1

【特許請求の範囲】

【請求項１】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する通信手段を備えた電子機器であって、

第１の状態と第２の状態を切り換え可能なスイッチと、

このスイッチが第１の状態に設定されている場合には、上記特定の識別コードによる認証を禁止する認証禁止手段と、

上記スイッチが第２の状態に設定されている場合には、上記特定の識別コードによる認証を許可する認証許可手段とを具備したことを特徴とする電子機器。

【請求項２】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを検知する時間検知手段と、

この時間検知手段により上記スイッチが第２の状態に設定されてから所定時間経過したことが検知された場合には、上記特定の識別コードによる認証を禁止する制御手段とを具備したことを特徴とする請求項１記載の電子機器。

【請求項３】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

他の機器との間で接続を行うための各種管理情報を記憶する管理情報記憶手段と、

第１の状態と第２の状態を切り換え可能なスイッチと、

このスイッチが第１の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を禁止する変更禁止手段と、

上記スイッチが第２の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を許可する変更許可手段とを具備したことを特徴とする電子機器。

【請求項４】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを検知する時間検知手段と、

この時間検知手段により上記スイッチが第２の状態に設定されてから所定時間経過したことが検知された場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を禁止する制御手段と、

を具備したことを特徴とする請求項３記載の電子機器。

【請求項５】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

リンクの張られた他の機器それぞれの機器コードを記憶する機器コード記憶手段と、

他の機器から接続要求があったときに、当該機器の機器コードが上記機器コード記憶手段に記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とを対応付けて記憶する認証エラー記憶手段と、

この認証エラー記憶手段に記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求を拒否する制御手段とを具備したことを特徴とする電子機器。

【請求項６】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

このリンク情報登録手段によるリンク情報の登録機器数が許容件数を越えた場合に所定の規則に従って不要と判定される機器のリンク情報を削除する削除手段とを具備したことを特徴とする電子機器。

【請求項７】　上記リンク情報登録手段は、各機器それぞれのリンク情報に対応付けて、各機器それぞれの最終接続時刻を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その最終接続時刻の最も古い機器のリンク情報を削除することを特徴とする請求項６記載の電子機器。

【請求項８】　上記リンク情報記憶手段は、各機器それぞれのリンク情報に対応付けて、その登録時刻を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その登録時刻の最も古い機器のリンク情報を削除することを特徴とする請求項６記載の電子機器。

【請求項９】　上記リンク情報記憶手段は、各機器それぞれのリンク情報に対応付けて、各機器それぞれの接続回数を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その接続回数の最も少ない機器のリンク情報を削除することを特徴とする請求項６記載の電子機器。

【請求項１０】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

上記特定の識別コードを記憶する識別コード記憶手段と、

他の機器から接続要求があったときに当該機器に対して上記識別コード記憶手段に記憶された特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリン

ク情報を作成するリンク情報作成手段と、
このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、
上記識別コード記憶手段に記憶された特定の識別コードが変更された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報を削除する削除手段とを具備したことを特徴とする電子機器。

【請求項１１】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する電子機器であって、
上記他の機器と接続するための交換可能な無線通信ユニットと、
この無線通信ユニットの固有の識別コードを記憶するユニットコード記憶手段と、
他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行う認証手段と、
この認証手段によって認証可と判定された機器とのリンク情報を上記ユニットコード記憶手段に記憶された無線通信ユニットの識別コードに基づき作成するリンク情報作成手段と、
このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、
上記無線通信ユニットが交換された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報を削除する削除手段とを具備したことを特徴とする電子機器。

【請求項１２】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する通信手段を備えた電子機器に用いられる接続制御方法であって、
上記電子機器の本体に第１の状態と第２の状態を切り換え可能なスイッチを設けておき、
このスイッチが第１の状態に設定されている場合には、上記特定の識別コードによる認証を禁止し、
上記スイッチが第２の状態に設定されている場合には、上記特定の識別コードによる認証を許可することを特徴とする接続制御方法。

【請求項１３】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを検知したか否かを判断し、
上記スイッチが第２の状態に設定されてから所定時間経過した場合には、上記特定の識別コードによる認証を禁止することを特徴とする請求項１２記載の接続制御方法。

【請求項１４】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、
他の機器との間で接続を行うための各種管理情報を記憶したメモリを備え、
上記電子機器の本体に第１の状態と第２の状態を切り換え可能なスイッチを設けておき、

第１の状態と第２の状態を切り換え可能なスイッチと、
このスイッチが第１の状態に設定されている場合には、上記メモリに記憶されている各種管理情報の変更を禁止し、
上記スイッチが第２の状態に設定されている場合には、上記メモリに記憶されている各種管理情報の変更を許可することを特徴とする接続制御方法。

【請求項１５】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを判断し、
上記スイッチが第２の状態に設定されてから所定時間経過した場合には、上記メモリに記憶されている各種管理情報の変更を禁止することを特徴とする請求項１４記載の接続制御方法。

【請求項１６】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、
リンクの張られた他の機器それぞれの機器コードを第１のメモリに記憶しておき、
他の機器から接続要求があったときに、当該機器の機器コードが上記第１のメモリに記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証を行い、
この認証により認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とを対応付けて第２のメモリに記憶し、
この第２のメモリに記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求を拒否することを特徴とする接続制御方法。

【請求項１７】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、
他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行い、
この認証によって認証可と判定された機器とのリンク情報を作成し、
このリンク情報を該当機器と対応付けてメモリに登録し、
このメモリによるリンク情報の登録機器数が許容件数を越えた場合に所定の規則に従って不要と判定される機器のリンク情報を削除することを特徴とする接続制御方法。

【請求項１８】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、
上記特定の識別コードを第１のメモリに記憶しておき、
他の機器から接続要求があったときに当該機器に対して上記第１のメモリに記憶された特定の識別コードによる認証を行い、
この認証によって認証可と判定された機器とのリンク情報を作成し、

このリンク情報を該当機器と対応付けて第２のメモリに登録し、
上記第１のメモリに記憶された特定の識別コードが変更された場合には、上記第２のメモリに登録されたすべてのリンク情報を削除することを特徴とする接続制御方法。
【請求項１９】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要し、上記他の機器と接続するための交換可能な無線通信ユニットを備えた電子機器の接続制御方法であって、
上記無線通信ユニットの固有の識別コードを第１のメモリに記憶しておき、
他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行い、
この認証によって認証可と判定された機器とのリンク情報を上記メモリに記憶された無線通信ユニットの識別コードに基づき作成し、
このリンク情報を該当機器と対応付けて第２のメモリに登録し、
上記無線通信ユニットが交換された場合には、上記第２のメモリに登録されたすべてのリンク情報を削除することを特徴とする接続制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、他の機器との間でデータ通信を行う無線通信機能を備えた電子機器及び接続制御方法に関する。
【０００２】
【従来の技術】近年、ＩｒＤＡ、Ｂｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ等のパーソナルエリアの無線通信システムが注目されている。特に、ＢｌｕｅｔｏｏｔｈやＨｏｍｅＲＦは、ＩｒＤＡのような赤外線通信方式と比較して、指向性がない、透過性が高いなどの長所を有しており、今後の発展、普及が大いに期待されている。なお、Ｂｌｕｅｔｏｏｔｈは、近距離の無線通信規格であり、２．４ＧＨｚ帯のＩＳＭ（Industrial Science Medical）バンドを用いて１０ｍ以内あるいは１００ｍ以内の無線通信を実現するものである。
【０００３】Ｂｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ等の無線通信システムは、同時に複数の機器との接続が可能である他に、ＩｒＤＡのような赤外線通信方式と比較して伝送距離が例えば１０～１００ｍと比較的長いということも大きな特徴の一つである。これは使い勝手の向上という利点もあるが、その反面、無線により外部から容易にアクセスできるため、無線通信システムのセキュリティ、秘話性の確保等に関しては十分に注意する必要がある。
【０００４】一般的な無線通信システムのセキュリティ方式としては、特許第２８７２９９６号の公報に記載されている方式が知られている。これは、電子鍵と無線端末装置からなるセキュリティシステムにおいて、セキュリティを強化するために、同一鍵の連続使用を禁止し、紛失や盗難に対しての安全性を高めたものである。
【０００５】また、Ｂｌｕｅｔｏｏｔｈでは、以下のようなユーザ認証によるセキュリティ方式が採用されている。
【０００６】Ｂｌｕｅｔｏｏｔｈにおけるユーザ認証は、機器に設定するユニークな認証パスワードと、この認証パスワード及び機器固有のＩＤ（ＩＥＥＥが管理、発番する４８ビットのアドレス）等により作成される暗号鍵との２つにより管理されている。上記認証パスワードはＰＩＮ（Personal Identification Number）コードと呼ばれ、任意の文字列で構成される。上記暗号鍵はリンクキーと呼ばれ、ユーザ認証の他にデータの暗号化などにも用いられる。
【０００７】今、機器Ａが機器Ｂに対してアクセスする場合を考える。
【０００８】機器Ａと機器Ｂが初めて接続される状況においては、機器Ａは機器ＢのＰＩＮコードを入力する必要がある。機器Ａから入力されたＰＩＮコードが正しいと判定された場合には、機器Ｂは認証可としてリンクを開設して接続を許可する。このとき、機器Ｂは自身のＰＩＮコード及び機器ＡのＩＤに乱数を掛け合わせるなどして機器Ａのリンクキーを作成し、これを機器ＡのＩＤと共にリンクキーテーブルに保存しておく。なお、リンクキーを作成する場合に、各機器間で互いにリンクキーを交換する相手のＰＩＮコードや自身のＩＤも用いる。
【０００９】一方、機器Ａが以前に機器Ｂに接続されたことがあれば、既に機器Ａのリンクキーが上記リンクテーブルに登録されているので、ＰＩＮコードの入力を省いて、上記リンクキーによる認証を行う。
【００１０】
【発明が解決しようとする課題】Ｂｌｕｅｔｏｏｔｈを利用した機器として様々なものがあり、その１つとして、モデムアクセスポイントと呼ばれる回線接続機器がある。このモデムアクセスポイントは公衆回線への接続機能を備えたものであり、これにＢｌｕｅｔｏｏｔｈの通信機能を付加すれば、他のＢｌｕｅｔｏｏｔｈ対応機器との間で無線による接続が可能となる。したがって、外部機器からモデムアクセスポイントに無線によりアクセスすれば、外部機器側ではモジュラーケーブルの接続を必要とせずに、公衆回線に接続してインターネット等の利用を受けることができる。この場合、モデムアクセスポイントへのアクセスには、上述したＰＩＮコードまたはリンクキーによる認証が行われており、認証可と判定された外部機器のみがモデムアクセスポイントへの接続が許される。
【００１１】しかしながら、モデムアクセスポイントのＰＩＮコードが何らかの手段で本来の使用者以外の者に知られた場合、そのＰＩＮコードを使用してモデムアク

セスポイントに不正アクセスする可能性がある。モデムアクセスポイントの場合には、公衆回線の接続によって回線使用料金が生じるため、不正アクセスは重大な問題となる。

【0012】また、通常、モデムアクセスポイントは目立たない場所に設置され、かつ、電源が常時ONになっていることが多い。このため、管理者が知らないうちに、外部からモデムアクセスポイントに不正アクセスする可能性が高い。

【0013】本発明は上記のような点を解決するためになされたもので、他の機器からの不正アクセスを防止してセキュリティを確保することのできる電子機器及び接続制御方法を提供することを目的とする。

【0014】

【課題を解決するための手段】すなわち、本発明の請求項1に係る電子機器では、他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、第1の状態と第2の状態を切り換え可能なスイッチが第1の状態に設定されている場合には、上記特定の識別コードによる認証が禁止され、また、上記スイッチが第2の状態に設定されている場合には、上記特定の識別コードによる認証が許可されるので、他の機器のユーザは、上記特定の識別コードを知っていても、上記スイッチを第1の状態に設定操作しない限り、当該機器とのリンクを張ることができないことになる。

【0015】また、本発明の請求項2に係る電子機器では、前記請求項1に係る電子機器にあって、上記スイッチが第2の状態に設定されてから所定時間経過したことが検知された場合には、上記特定の識別コードによる認証は禁止されるので、上記スイッチが第2の状態に設定されたままでも、所定時間経過の後は他の機器とのリンクを張ることができないようになる。

【0016】また、本発明の請求項3に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、他の機器との間で接続を行うための各種管理情報を記憶する管理情報記憶手段を有し、第1の状態と第2の状態を切り換え可能なスイッチが第1の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更が禁止され、また、上記スイッチが第2の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更が許可されるので、他の機器の不正ユーザがこの電子機器と接続できても、上記スイッチを第1の状態に設定操作しない限り、上記他の機器との接続のための各種管理情報の変更操作はできないことになる。

【0017】また、本発明の請求項4に係る電子機器では、前記請求項3に係る電子機器にあって、上記スイッチが第2の状態に設定されてから所定時間経過したことが検知された場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更は禁止されるので、上記スイッチが第2の状態に設定されたままでも、所定時間経過の後は上記他の機器との接続のための各種管理情報の変更操作はできないないようになる。

【0018】また、本発明の請求項5に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、リンクの張られた他の機器それぞれの機器コードを記憶する機器コード記憶手段を有し、他の機器から接続要求があったときに、当該機器の機器コードが前記機器コード記憶手段に記憶されてない場合には、当該機器に対して上記特定の識別コードによる認証が行われ、認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とが対応付けられて認証エラー記憶手段に記憶される。そして、この認証エラー記憶手段に記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求が拒否されるので、同一機器からの不正な接続の試みはできないようになる。

【0019】また、本発明の請求項6に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、このリンク情報登録手段によるリンク情報の登録機器数が許容件数を越えた場合には、その登録リンク情報のうち、例えば最終接続時刻の最も古い機器のリンク情報（請求項7）、又は登録時刻の最も古い機器のリンク情報（請求項8）、又は接続回数の最も少ない機器のリンク情報（請求項9）という不要なリンク情報が判定されて削除されるので、新たな接続機器とのリンク情報を接続可能性の低い機器のリンク情報と代えて登録できることになる。

【0020】また、本発明の請求項10に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、上記特定の識別コードを記憶する識別コード記憶手段を有し、他の機器から接続要求があったときに当該機器に対して上記識別コード記憶手段に記憶された特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、上記識別コード記憶手段に記憶された特定の識別コードが変更された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報が削除されるので、上記特定の識別コードの書き換え後は当該新たな識別コードを知らないユーザによって他の機器との間でリンクが張られるのを防止できることになる。

【0021】また、本発明の請求項11に係る電子機器

では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、上記他の機器と接続するための交換可能な無線通信ユニットと、この無線通信ユニットの固有の識別コードを記憶するユニットコード記憶手段を有し、他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が上記ユニットコード記憶手段に記憶された無線通信ユニットの識別コードに基づき作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、上記無線通信ユニットが交換された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報が削除されるので、上記無線通信ユニットの交換後はそのユニット固有の識別コードに基づくリンク情報を作成し登録し直さないと、他の機器とのリンクが張れないことになる。

【００２２】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。

【００２３】図１は本発明の一実施形態に係る無線通信システムの外観構成を示す斜視図である。図１では、公衆回線の接続機能を備えた回線接続機器（以下、アクセスポイントと称す）１０と、このアクセスポイント１０との間で無線通信を行うパーソナルコンピュータ（以下、パソコンと称す）１００が示されている。

【００２４】アクセスポイント１０およびパソコン１００には、無線通信カードとして、Ｂｌｕｅｔｏｏｔｈの無線通信規格に従ったＰＣカード（以下、ＢＴ－ＰＣカードと称す）２０が脱着自在に装着されている。アクセスポイント１０およびパソコン１００は、このＢＴ－ＰＣカード２０を装着することで、互いに無線によるデータ通信が可能となる。

【００２５】パソコン１００は、ここではアクセスポイント１０にアクセスする外部機器として用いられる。このパソコン１００の本体１１４には、キーボード１１２や液晶表示パネル１１６、カードスロット１１８が設けられている。

【００２６】アクセスポイント１０は、モジュラケーブル１２を介して公衆回線１１に接続され、パソコン１００から無線送信されたデータを公衆回線１１に転送すると共に公衆回線１１から入力されたデータをパソコン１００に無線送信する。

【００２７】図２乃至図６にアクセスポイント１０の構成を示す。

【００２８】図２はアクセスポイント１０の分解斜視図、図３はアクセスポイント１０を縦置きで使用した状態を示す斜視図、図４はアクセスポイント１０の背面側を示す斜視図、図５はアクセスポイント１０を横置きで使用した状態を示す斜視図、アクセスポイント１０の底面側を示す斜視図である。

【００２９】図２乃至図６に示すように、アクセスポイント１０は、例えば合成樹脂によって形成されたほぼ矩形状の機器本体１４を備えている。この機器本体１４は、僅かに湾曲した前面１４ａ、この前面と対向したほぼ平坦な背面１４ｂ、対向する一対の側面１４ｃ、上面１４ｄ、および底面１４ｅを有している。そして、機器本体１４の底面１４ｅおよび背面１４ｂはそれぞれ第１および第２設置面を構成している。

【００３０】アクセスポイント１０は、図３および図４に示すように、底面１４ｅを机面上等に載置することにより機器本体１４を縦置きとして使用し、あるいは、図５に示すように、背面１４ｂを机面上等に載置することにより機器本体１４を横置きとして使用することができる。また、背面１４ｂには、ビンやフック等を掛けるための２つの係合凹所１６が形成され、これらの係合凹所１６を利用することにより、機器本体１４をその背面が壁と対向した状態で壁掛け式としても使用することができる。

【００３１】機器本体１４の一方の側面１４ｃには、押しボタン式の電源スイッチ１８が設けられている。他方の側面１４ｃには、ＲＳ２３２Ｃコネクタ２２および電源接続用のＡＣアダプタ端子２３が設けられている。また、機器本体１４の前面１４ａには、アクセスポイント１０の動作状態を示す表示部として、複数のＬＥＤ２４が並んで設けられている。動作状態としては、例えば、電源オン（POWER）、送信（SD）、受信（RD）、オフフック（OH）、後述するＢＴ－ＰＣカード２０のスタンバイ／アクティブ（STB/ACT）状態等を表示する。

【００３２】機器本体１４の上面１４ｄには、着脱自在な透明カバー１５と、後述するカードスロット２６のカード挿入口２８およびイジェクトボタン３０が設けられている。また、図６から分かるように、底面１４ｅには、アクセスポイント１０を公衆回線１１に接続するためのモジュラケーブル１２を接続可能な２つのモジュラジャック３２、左右一対のスライドスイッチ３４ａ、３４ｂ、１つのロータリスイッチ３５が設けられている。

【００３３】底面１４ｅには、その周縁部に沿ってスカート部３６が立設され、その一部には切欠３７が形成されている。このスカート部３６は、機器本体１４を縦置きとして使用する際に脚部として機能する。上記モジュラジャック３２に接続されたモジュラケーブル１２は、切欠３７を通して外部に引き出される。従って、モジュラジャック３２にモジュラケーブル１２を接続した状態で機器本体１４を縦置きとして使用する場合でも、モジュラケーブル１２が邪魔になることなく、スカート部３６により機器本体１４を安定して支持することができる。

【００３４】機器本体１４内には、保持部として機能するカードスロット２６が設けられ、このカードスロットのカード挿入口２８は機器本体の上面１４ｄに開口して

いる。そして、このカードスロット２６には、カード挿入口２８を通して、ＢＴ－ＡＣカード２０を脱着自在に装着可能となっている。

【００３５】次に、ＢＴ－ＰＣカード２０の構成について説明する。

【００３６】図７はＢＴ－ＰＣカード２０の斜視図、図８はＢＴ－ＰＣカード２０の分解斜視図である。

【００３７】図７および図８に示すように、ＢＴ－ＰＣカード２０は、ＰＣＭＣＩＡの規格に準拠したカード本体４０と、カード本体の一端側から突出している共にＢＴ規格に準拠した送受信部４２とを備えている。カード本体４０は、合成樹脂からなるほぼ矩形状の枠体４３を有する。この枠体４３は、カード本体４０内のカード基板４４の周縁部を支持している。カード基板４４の一端にはコネクタ４５が取り付けられ、また、カード基板の他端部はカード本体４０から突出している。

【００３８】カード基板４４の一方の表面、ここでは上面４４ａ上には、複数の電子部品４６が実装されている。また、カード基板４４の他端部上面には、送受信部４２を構成するアンテナ部４６、送受信時に点灯するＬＥＤ４７およびヘッドフォン、マイクロフォン等を接続するためのヘッドセット部４８が設けられている。

【００３９】そして、カード基板４４の上面および下面は、枠体４３に嵌合された一対の金属カバー５０ａ、５０ｂにより、他端部を除いて覆われている。

【００４０】また、送受信部４２は合成樹脂からなるキャップ５１を有し、このキャップ５１はカード本体４０の他端に嵌合され、カード基板４４の他端部、およびこの他端部上面に実装されたアンテナ部４６、ＬＥＤ４７、ヘッドセット部４８を覆っている。

【００４１】上記ＢＴ－ＰＣカード２０において、コネクタ４５が設けられている前端はカードスロット２６に対して挿入側端となる。そして、枠体４３の一方の側壁前端には、カード本体４０の上面、側面、前端面に開口した第１ガイド溝５２ａが形成され、また、枠体４３の他方の側壁前端には、カード本体４０の側面および前端面のみに開口した第２ガイド溝５２ｂが形成されている。これらの第１および第２ガイド溝５２ａ、５２ｂは、ＢＴ－ＰＣカード２０をカードスロット２６に装着する際、ＢＴ－ＰＣカード２０の表裏の向きを規制する。

【００４２】パソコン１００に装着されるＢＴ－ＰＣカード２０も同様の構成であり、図１に示すようにパソコン１００の側面部に設けられたカードスロット１１８を介して装着される。

【００４３】このような構成のＢＴ－ＰＣカード２０をアクセスポイント１０、パソコン１００にそれぞれ装着することで、アクセスポイント１０とパソコン１００との間でＢｌｕｅｔｏｏｔｈの無線通信規格に従ったデータ通信が可能となる。

【００４４】ところで、パソコン１００がアクセスポイント１０にアクセスする場合に、アクセスポイント１０とパソコン１００が初めて接続される状況においては、パソコン１００はアクセスポイント１０のＰＩＮコードを入力する必要がある。アクセスポイント１０は、パソコン１００から入力されたＰＩＮコードが正しければリンクを開設して接続を許可する。このとき、アクセスポイント１０はパソコン１００のＩＤや自身のＰＩＮコードなどを元にリンクキーを作成し、次回パソコン１００から接続要求があったときには、このリンクキーによる認証を行うことになる。

【００４５】アクセスポイント１０のＰＩＮコード（認証パスワード）は予め接続が許可された使用者にのみ知らされているものである。しかし、何らかの手段（例えばコード解読専用のソフトウェアを使用するなどして）で本来の使用者以外の者に知られると、そのＰＩＮコードを用いてアクセスポイント１０に不正アクセスして、公衆回線１１を無断で使用する問題がある。

【００４６】以下では、このような不正アクセスを防止することを主旨として説明する。

【００４７】図９は本発明の無線通信システムの構成を示すブロック図であり、上記図１の構成と対応しており、アクセスポイント１０とパソコン１００とで無線通信システムを構成してことが示されている。

【００４８】ここで、本実施形態では、図１０に示すようにアクセスポイント１０の裏面など、目立たないの場所にスライドスイッチ３４ａ、３４ｂが設けられている。これらのスライドスイッチ３４ａ、３４ｂは２位置間を切り換え可能なスイッチであり、禁止モードと許可モードの切り換え操作を行うためのものであり。スライドスイッチ３４ａはＰＩＮコードによる認証動作（新規機器の登録動作）を禁止／許可し、スライドスイッチ３４ｂはセキュリティ情報のメンテナンス動作（ＰＩＮコードやリンクキーの変更動作）を禁止／許可する。

【００４９】スライドスイッチ３４ａ、３４ｂの操作は基本的にはアクセスポイント１０の管理者が行い、通常はスライドスイッチ３４ａ、３４ｂ共に禁止状態に設定しておく。そして、アクセスポイント１０に新規機器の登録を行う場合に、管理者がスライドスイッチ３４ａを操作して許可状態に切り換える。

【００５０】このように、本来の使用者が新たに接続を行う場合にスライドスイッチ３４ａを許可状態に切り換え、普段は禁止状態としておけば、本来の使用者以外の者がアクセスポイント１０のＰＩＮコードを入力して不正アクセスすることを防止することができる。

【００５１】また、アクセスポイント１０のＰＩＮコードの変更や、各機器のリンクキーの削除といったモデムアクセスポイント１０内に記憶されたセキュリティ情報のメンテナンスは、外部（既に登録されている機器）からコマンドを入力することにより実行できる。このよう

なセキュリティ情報のメンテナンスをスライドスイッチ３４ｂが許可状態になっているときのみ実行可能とすることで、アクセスポイント１０内のセキュリティ情報を勝手にアクセスして変更してしまうことを防止する。

【００５２】なお、スライドスイッチ３４ａ、３４ｂとは別に、図１１に示すようなロータリスイッチ３５を用いることでも良い。このロータリスイッチ３５は、少なくとも４つの位置間を切換え可能なものとし、第１の位置でＰＩＮコードによる認証動作（新規機器の登録動作）とセキュリティ情報のメンテナンス動作（ＰＩＮコードやリンクキーの変更動作）の両方を禁止し、第２の位置でＰＩＮコードによる認証動作のみを許可、第３の位置でセキュリティ情報のメンテナンス動作のみを許可、第４の位置でＰＩＮコードによる認証動作とセキュリティ情報のメンテナンス動作の両方を許可する。

【００５３】図１２にスライドスイッチ３４ａ、３４ｂとロータリスイッチ３５との対応関係を示す。図中のＳＷ１はスライドスイッチ３４ａ、ＳＷ２はスライドスイッチ３４ｂを示し、ＯＦＦは禁止状態、ＯＮは許可状態を示している。また、１～４はロータリスイッチ３５の切換え位置を示している。

【００５４】このようなスライドスイッチ３４ａ、３４ｂとロータリスイッチ３５との対応関係を表したテーブルをアクセスポイント１０に持たせておくことで、スライドスイッチ３４ａ、３４ｂまたはロータリスイッチ３５にてアクセスポイント１０の動作状態を切り換えることができる。ただし、ロータリスイッチ３５はスライドスイッチ３４ａ、３４ｂに比べて操作しずらいため、スライドスイッチ３４ａ、３４ｂを用いてアクセスポイント１０の動作状態を切り換えることの方が好ましい。以下では、スライドスイッチ３４ａ、３４ｂを用いてアクセスポイント１０の動作状態を切り換えるものとして説明する。

【００５５】図１３はアクセスポイント１０とＢＴ－ＰＣカード２０の回路構成を示すブロック図である。

【００５６】図１３に示すように、アクセスポイント１０は、アクセスポイント全体の動作を制御するＣＰＵ７２を備えている。このＣＰＵ７２にはＬＥＤ２４、スイッチ群３４ａ、３４ｂ、３５、ＰＣカードインターフェースとしてのコネクタ６０、ＲＯＭ７３、ＲＡＭ７４、不揮発性メモリ７５、ＲＴＣ（Ｒｅａｌ　ＴｉｍｅＣｌｏｃｋ）回路７６などが接続される。また、ＡＣアダプタ端子２３から供給される電源は、電源供給部７７を介してＣＰＵ７２に供給される。

【００５７】更に、アクセスポイント１０は、モジュラケーブル１２およびモジュラジャック３２を介して公衆回線１１に接続されるモデム部７０を備えている。このモデム部７０およびＲＳ２３２Ｃコネクタ２２は、切換えスイッチ７８を介してＣＰＵ７２に接続されている。なお、モデム部７０およびモジュラジャック３０は送受信部として機能する。

【００５８】ＲＯＭ７３は、無線通信および公衆回線１１との通信プロトコル等を格納している。ＲＡＭ７４は、アクセスポイント１０の動作プログラム、デバイスドライバおよび無線通信プロトコルを含むドライバソフトを格納している。

【００５９】また、このＲＡＭ７４には、ここではＰＩＮコードの認証動作を制御する第１の動作制御情報、セキュリティ情報のメンテナンス動作を制御する第２の動作制御情報、基準時刻情報ＴＭを格納しておくための各種格納部７４ａ～７４ｃなどが設けられている。

【００６０】不揮発性メモリ７５としては、例えばＥＥＰＲＯＭが用いられる。この不揮発性メモリ７５には、後述するリンクテーブルＴ１および認証エラーテーブルＴ２が設けられていると共に、自身のＩＤ（ＢＴ－ＰＣカード２０に登録されている）を保持しておくためのＩＤ格納部７５ａや、自身のＰＩＮコード（ユーザが任意に作成した認証用パスワード）を保持しておくためのパスワード格納部７５ｂなどが設けられている。

【００６１】ＲＴＣ回路７６は、現在の時刻を計時するための回路である。

【００６２】モデム部７０は、ＢＴ－ＰＣカード２０から入力されたデジタルデータをアナログデータに変換し、モジュラジャック３２を介して公衆回線１１に転送し、また、モジュラジャック３２を介して公衆回線１１から入力されたアナログデータをデジタルデータに変換し、ＣＰＵ７２に転送する。

【００６３】ＲＣ２３２Ｃコネクタ２２は、図示せぬＲＳ２３２Ｃケーブルを介してパソコン１００等の外部機器とアクセスポイント１０とをシリアル接続するために設けられている。例えば、ＲＣ２３２Ｃコネクタ２２およびＲＳ２３２Ｃケーブルを介してアクセスポイント１０にＩＳＤＮターミナルアダプタに接続し、ＢＴ－ＰＣカード２０から入力されたデジタルデータをそのまま伝送することも可能である。

【００６４】切換えスイッチ７８は、モデム部７０およびモジュラジャック３２による公衆回線１１との接続と、ＲＳ２３２Ｃコネクタ２２による他の電子機器との接続とを切り換える。

【００６５】一方、このアクセスポイント１０に装着されるＢＴ－ＰＣカード２０は、ＢＴ規格の無線モジュールとして、アンテナ部４６、ＲＦ部８０、ベースバンド部８１、メモリ８２、水晶発振部８３、ヘッドセット部４８、ＡＤ／ＤＡ変換部８４、ＬＥＤ４７を備えている。

【００６６】ＢＴ－ＰＣカード２０とアクセスポイント１０とのデータの送受信はコネクタ４５を介して行う。アンテナ部４６は、無線通信を実行するための電波の送信、受信を行い、使用する周波数帯域はＢＴ規格の２．４～２．５ＧＨｚとなっている。ＲＦ部８０は、使用す

る所定の無線電波の周波数で通信が実行可能な信号処理を行う。

【００６７】また、ベースバンド部８１は、アンテナ部４６、ＲＦ部８０を介して入力されたデータをデジタル処理し、アクセスポイント１０で処理可能なデータに変換してメモリ８２に格納し、アクセスポイントとの間でデータの授受を行う。なお、ここではメモリ８２にＩＤが予め記憶されているものとする。実際には、図示せぬ書き換え不可メモリに予めＢＴ－ＰＣカード２０に割り付けられたＩＤが記憶されており、ＢＴ－ＰＣカード２０装着時にこのＢＴ－ＰＣカード２０のＩＤが機器固有の識別情報として不揮発性メモリ７５に書き込まれる。

【００６８】ＬＥＤ４７は、例えばデータの送受信時に点灯する。水晶発振部８３は、ＲＦ部８０で使用する基準波を供給する。ヘッドセット部４８は、ヘッドフォンとマイクロフォンとを有するヘッドセットを接続し、音声信号の入出力を行う。また、ＡＤ／ＤＡ変換部８４は、ヘッドセット部４８から入力されたアナログの音声信号をデジタルデータに変換すると共に、アクセスポイント１０からベースバンド部８１を介して入力されたデジタルの音声信号をアナログデータに変換してヘッドセット部４８に出力する。

【００６９】図１４はである。アクセスポイント１０に外部機器として接続されるパソコン１００とＢＴ－ＰＣカード２０の回路構成を示すブロック図。

【００７０】パソコン１００には、図１に示すようにキーボード１１２が設けられた本体１１４と、この本体１１４に開閉自在に設けられた液晶表示パネル１１６とを有している。本体１１４にはカードスロット１１８が設けられ、このカードスロット１１８にはＢＴ－ＰＣカード２０が脱着自在に装着されている。カードスロット１１８の構成は上述したアクセスポイント１０のカードスロット２６とほぼ同一である。また、ＢＴ－ＰＣカード２０はアクセスポイント１０と共通であり、その内部構成は図１３と同様であるため、ここではその説明を省略する。

【００７１】また、パソコン１００には、ＢＴ－ＰＣカード２０との間でデータの送受信を行うＰＣＭＣＩＡ規格のインターフェースコネクタ１２０と、パソコン全体の動作を制御するＣＰＵ１２２を備えている。ＣＰＵ１２２には、ＵＳＢ１２４、ＲＯＭ１２６、ＲＡＭ１２８などが接続されている。

【００７２】ＵＳＢ１２４は、例えばアクセスポイント１０とＲＳ２３２Ｃコネクタ２２を介してシリアル接続する際に使用する。ＲＯＭ１２６には、プログラム等のデータが記憶されている。ＲＡＭ１２８には、ＣＰＵ１２２の処理動作に必要な各種のデータが記憶される。また、このＲＡＭ１２８には、パソコン１００に設定されたＰＩＮコード（ユーザが任意に作成した認証パスワード）や、ＢＴ－ＰＣカード２０から読み込んだＩＤを格納したおくための各種データ格納部が設けられている。

【００７３】次に、アクセスポイント１０が管理しているリンクテーブルＴ１および認証エラーテーブルＴ２の構成について説明する。

【００７４】図１５はリンクテーブルＴ１の構成を示す図である。

【００７５】リンクテーブルＴ１には、各機器に固有のＩＤ（アドレス）、そのＩＤなどを元に作成されたリンクキー、最終接続時刻、データ有無フラグが登録される。

【００７６】上述したように、アクセスポイント１０では、新たな機器（リンクテーブルＴ１に未登録の機器）から接続要求があったときにはＰＩＮコードによる認証を行い、認証ＯＫの場合にその機器のＩＤなどを元にリンクキーを作成し、そのリンクキーをＩＤと共にリンクテーブルＴ１に登録する。また、このときの接続時刻をＲＴＣ回路７６から取得してリンクテーブルＴ１に登録しておく。上記接続時刻は機器接続時にその都度更新される。なお、データ有無フラグは当該レコード欄にデータが登録されているか否かを示すものである。

【００７７】図１６は認証エラーテーブルＴ２の構成を示す図である。

【００７８】認証エラーテーブルＴ２は、各機器に固有のＩＤ（アドレス）、認証エラー回数、最終接続時刻、データ有無フラグが登録される。

【００７９】アクセスポイント１０は、ＰＩＮコードによる認証の際に認証エラーと判定された機器に対し、その機器のＩＤと認証エラー回数とを対応付けて認証エラーテーブルＴ２に登録しておく。認証エラー回数の初期値は「１」であり、機器が認証エラーと判定される毎に更新される。また、このときの接続時刻をＲＴＣ回路７６から取得して認証エラーテーブルＴ２に登録しておく。上記接続時刻は機器接続時にその都度更新される。なお、データ有無フラグは当該レコード欄にデータが登録されているか否かを示すものである。

【００８０】リンクテーブルＴ１及び認証エラーテーブルＴ２の登録数は不揮発性メモリ７５の容量に応じて決められており、図１５の例ではリンクテーブルＴ１の最大登録件数はＮ件、図１６の例では認証エラーテーブルＴ２の最大登録件数はＭ件である。

【００８１】次に、本システムの動作について説明する。

【００８２】ここでは、アクセスポイント１０に対する不正アクセスを防止するための処理として、（ａ）スイッチによる動作状態の切り換え処理、（ｂ）外部機器との接続処理、（ｃ）セキュリティ情報のメンテナンス処理、（ｄ）接続時の認証エラー処理に分けて説明する。

【００８３】（ａ）スイッチによる動作状態の切り換え処理

上述したように、アクセスポイント１０の裏面には、ア

クセスポイント１０の動作状態を切換えるためのスライドスイッチ３４ａ、３４ｂが設けられている。スライドスイッチ３４ａはＰＩＮコードによる認証動作を禁止状態または許可状態とするものであり、スライドスイッチ３４ｂはセキュリティ情報のメンテナンス動作を禁止状態または許可状態とするものである。

【００８４】ここで、スライドスイッチ３４ａによる動作状態の切換え処理について説明する。

【００８５】図１７はアクセスポイント１０に設けられたスライドスイッチ３４ａによる動作状態の切換え処理を示すフローチャートである。なお、図１７はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。また、図中ＳＷ１はスライドスイッチ３４ａのことである。

【００８６】アクセスポイント１０では、スライドスイッチ３４ａの状態を常に監視している。アクセスポイント１０は、スライドスイッチ３４ａが禁止状態から許可状態に切り換えられたことを検知すると（ステップＡ１１のＹｅｓ）、まず、図１３に示すＲＴＣ回路７６から現在時刻を取得し、この時刻を基準時刻情報ＴＭとしてＲＡＭ７４内の基準時刻格納部７４ｃにセットする（ステップＡ１２）。そして、ＰＩＮコードの認証動作を許可とする第１の動作制御情報をＲＡＭ７４内の第１の動作制御情報格納部７４ａにセットする（ステップＡ１３）。

【００８７】一方、アクセスポイント１０は、スライドスイッチ３４ａが許可状態から禁止状態に切り換えられたことを検知すると（ステップＡ１４のＹｅｓ）、ＰＩＮコードの認証動作を禁止とする第１の動作制御情報をＲＡＭ７４内の第１の動作制御情報格納部７４ａにセットする（ステップＡ１５）。

【００８８】また、スライドスイッチ３４ａが禁止状態から許可状態に切り換えられた後に、その切り換え時にセットされた基準時刻情報ＴＭと現在時刻との差が所定時間以上になると、つまり、スライドスイッチ３４ａが許可状態に切り換えられてから所定時間経過すると（ステップＡ１６のＹｅｓ）、アクセスポイント１０は、スライドスイッチ３４ａの状態に関係なく、ＰＩＮコードの認証動作を禁止とする第１の動作制御情報を第１の動作制御情報格納部７４ａにセットする（ステップＡ１７）。

【００８９】スライドスイッチ３４ｂについても同様である。

【００９０】すなわち、スライドスイッチ３４ｂが禁止状態から許可状態に切り換えられると、そのときの時刻が基準時刻情報ＴＭとしてＲＡＭ７４内の基準時刻格納部７４ｃにセットされると共に、セキュリティ情報のメンテナンス動作を許可とする第２の動作制御情報がＲＡＭ７４内の第２の動作制御情報格納部７４ｂにセットされる。一方、スライドスイッチ３４ｂが許可状態から禁止状態に切り換えられると、セキュリティ情報のメンテナンス動作を禁止とする第２の動作制御情報がＲＡＭ７４内の第２の動作制御情報格納部７４ｂにセットされる。

【００９１】更に、スライドスイッチ３４ｂが禁止状態から許可状態に切り換えられた後、その切り換え時にセットされた基準時刻情報ＴＭ（スライドスイッチ３４ａを管理するものとは別のものとする）と現在時刻との差が所定時間以上になると、つまり、スライドスイッチ３４ｂが許可状態に切り換えられてから所定時間経過すると、スライドスイッチ３４ｂの状態に関係なく、セキュリティ情報のメンテナンス動作を禁止とする第２の動作制御情報がＲＡＭ７４内の第２の動作制御情報格納部７４ｂにセットされる。

【００９２】なお、上記所定時間は例えば１０分程度が妥当であるが、その時間は予め決められていても良いし、アクセスポイント１０の管理者が任意に設定できるようにしても良い。

【００９３】（ｂ）外部機器との接続処理

次に、外部機器との接続処理について説明する。

【００９４】図１８はアクセスポイント１０における外部機器との接続処理の動作を示すフローチャートである。なお、図１８はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。

【００９５】例えば外部機器であるパソコン１００からアクセスポイント１０に対して、無線通信により接続要求が送られてくると、アクセスポイント１０は、まず、ＲＡＭ７４内の第１の動作制御情報格納部７４ａに格納された第１の動作制御情報に基づいて、ＰＩＮコードによる認証動作が許可されているか否かをチェックする（ステップＢ１１）。

【００９６】上述したように、スライドスイッチ３４ａが許可状態に切り換えられており、かつ、スライドスイッチ３４ａが許可状態に切り換えられてから所定時間経過していない場合に、第１の動作制御情報は許可を示している。また、スライドスイッチ３４ａが禁止状態に切り換えられているか、あるいは、スライドスイッチ３４ａが許可状態に切り換えられてから所定時間経過している場合に、第１の動作制御情報は禁止を示している。

【００９７】ＰＩＮコードによる認証動作が許可されていれば（ステップＢ１２のＹｅｓ）、アクセスポイント１０は接続要求先のパソコン１００が初めての接続か否かをパソコン１００に対するリンクキーの有無によってチェックする（ステップＢ１３）。すなわち、アクセスポイント１０が持つリンクテーブルＴ１には、これまでにアクセスポイント１０に接続された機器のＩＤとリンクキーとが登録されている。このリンクテーブルＴ１にパソコン１００に対するリンクキーがなければ、言い換えれば、リンクテーブルＴ１にパソコン１００のＩＤが登録されていなければ、パソコン１００は初めての接続

と判定される。

【００９８】ここで、アクセスポイント１０とパソコン１００とが初めて接続される状況においては（ステップＢ１３のＹｅｓ）、パソコン１００からアクセスポイント１０のＰＩＮコードを入力する必要がある。

【００９９】パソコン１００からＰＩＮコードが入力されると、アクセスポイント１０はこのＰＩＮコードによる認証を行う（ステップＢ１４）。上記ＰＩＮコードが正しい場合つまり不揮発性メモリ７５内のパスワード格納部７５ｂに格納された自身のＰＩＮコードと一致した場合には認証可と判定する（ステップＢ１５のＹｅｓ）。

【０１００】ここで、ＰＩＮコードによる認証動作について、図２２を参照して具体的に説明する。

【０１０１】今、機器Ａが機器Ｂに接続を行う場合を想定する。本実施形態では、機器Ａはパソコン１００、機器Ｂはアクセスポイント１０に相当する。また、図中のパスワードとは、アクセスポイント１０のＰＩＮコードのことである。

【０１０２】図２２に示すように、まず、機器Ａがコネクション要求（接続要求）を送信する（ステップＳ１）。機器Ｂは機器Ａからのコネクション要求を受信すると、この受信データを解析し、問題がない場合にはコネクション確立のメッセージを機器Ａに送信し（ステップＳ２）、しかる後に、機器Ａ－Ｂ間でコネクションが確立する（ステップＳ３）。なお、この場合のコネクションとは、通信の低位レイヤのコネクションを意味するもので、例えば「仮のネットワークアドレスが与えられた」という状況を意味するものとし、必ずしも上位アプリケーションのサービスを意味するものではない。

【０１０３】上記コネクションが確立した後、パスワードによる認証手続きが行なわれる。すなわち、機器Ｂは、上記コネクションが確立すると、機器Ａに認証要求を出力し、パスワードの入力を促す（ステップＳ４）。これにより、機器Ａのユーザは機器Ｂのパスワードを入力し、それを送信する（ステップＳ５）。

【０１０４】上記パスワードを受信した機器Ｂは、自機のパスワードと受信したパスワードとを照合する。照合結果が間違っていれば、パスワードが違う旨のメッセージを機器Ａに返すが、照合結果に問題がなければ認証を完了する（ステップＳ６）。

【０１０５】図１８に戻って、上記のようなＰＩＮコードによる認証動作が行われた結果、認証可と判定された場合に（ステップＢ１５のＹｅｓ）、アクセスポイント１０はリンクを開設し（ステップＢ１６）、パソコン１００に対するリンクキーを作成する（ステップＢ１７）。詳しくは、パソコン１００のＩＤを取得し、そのＩＤと自身のＰＩＮコードなどをアクセスポイント１０側で発生する乱数を掛け合わせるなどして、解読困難なリンクキーを作成する。そして、アクセスポイント１０は上記作成されたリンクキーをパソコン１００のＩＤと共にリンクテーブルＴ１に登録する（ステップＢ１８）。その際、ＲＴＣ回路７６から現在の時刻を取得し、そのときの時刻を最終接続時刻としてリンクテーブルＴ１に登録すると共に、データ有無フラグを「有」にセットしておく。

【０１０６】ここで、リンクテーブルＴ１に新たな機器のデータを登録する際に、リンクテーブルＴ１に空きがなければ（データ有無フラグがすべて有の状態）、最終接続時刻の最も古い機器のデータをリンクテーブルＴ１から削除して、そこに新たな機器のデータを登録するものとする。このように、接続される可能性の低い機器のリンクキーの代わりに新たに接続された機器のリンクキーを登録することで、不揮発性メモリ７５に設けられるリンクテーブルＴ１の登録件数（図１５の例ではＮ件）の中で新たな接続相手を優先してＰＩＮコードを効率的に管理でき、使い勝手を向上させることができる。

【０１０７】なお、例えば各機器の本機器に対するアクセス回数をリンクテーブルＴ１に記憶させておき、アクセス回数の最も少ない機器のデータを削除することでも良い。

【０１０８】また、各機器のリンクテーブルＴ１への登録時刻をリンクテーブルＴ１に記憶させておき、その登録時刻の最も古い機器のデータを削除することでも良い。

【０１０９】ＰＩＮコードによる認証がＯＫとされると、アクセスポイント１０とパソコン１００との接続が確立され、互いに無線によるデータ通信が可能となる（ステップＢ１９）。また、ＰＩＮコードによる認証がＮＧであった場合には（ステップＢ１５のＮｏ）、アクセスポイント１０はそのときの接続要求先であるパソコン１００との接続を拒否する。

【０１１０】一方、ＰＩＮコードによる認証動作が禁止されている場合（ステップＢ１２のＮｏ）あるいはパソコン１００が以前にアクセスポイント１０に接続されたことがある場合には（ステップＢ１３のＮｏ）、アクセスポイント１０はリンクキーによる認証を行う（ステップＢ２０）。この場合、接続要求先のパソコン１００が以前にアクセスポイント１０に接続されたことがあれば、パソコン１００に対するリンクキーがリンクテーブルＴ１に登録されているので、そのリンクキーを用いて認証を行うことができる。認証ＯＫであれば（ステップＢ２１のＹｅｓ）、アクセスポイント１０はパソコン１００との接続を確立する（ステップＢ１９）。また、ＰＩＮコードによる認証がＮＧであった場合には（ステップＢ２１のＮｏ）、アクセスポイント１０はそのときの接続要求先であるパソコン１００との接続を拒否する。

【０１１１】このように、ＰＩＮコードによる認証動作が許可されている場合のみ、新たな機器がアクセスポイント１０へのアクセスを試みることができる。したがっ

て、普段はスライドスイッチ３４ａの操作によりＰＩＮコードによる認証動作を禁止しておけば、本来の使用者以外の者がアクセスポイント１０のＰＩＮコードを何らかの手段で入手したとしても、アクセスポイント１０に対してアクセスすることはできないため、公衆回線１１が無断で使用するなどの不正行為を防ぐことができる。

【０１１２】また、アクセスポイント１０の管理者がスライドスイッチ３４ａを禁止状態に切り換えておくのを忘れたとしても、所定時間経過すると、スライドスイッチ３４ａの状態に関係なく、ＰＩＮコードによる認証動作が自動的に禁止されるため、アクセスポイント１０のセキュリティを強化することができる。

【０１１３】（ｃ）セキュリティ情報のメンテナンス処理

次に、セキュリティ情報のメンテナンス処理について説明する。

【０１１４】図１９はアクセスポイント１０におけるセキュリティ情報のメンテナンス処理の動作を示すフローチャートである。なお、図１９はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。

【０１１５】今、外部機器であるパソコン１００との接続が確立された状態で（ステップＣ１１）、パソコン１００からセキュリティ情報のメンテナンスコマンドが無線より送信されたものとする。セキュリティ情報のメンテナンスコマンドには、ＰＩＮコードの読み出しや書き換え、リンクテーブルＴ１の読み出しや削除などがある。

【０１１６】アクセスポイント１０は上記メンテナンスコマンドを受信すると、まず、ＲＡＭ７４内の第２の動作制御情報格納部７４ｂに格納された第２の動作制御情報に基づいて、セキュリティ情報のメンテナンス動作が許可されているか否かをチェックする（ステップＣ１２）。

【０１１７】上述したように、スライドスイッチ３４ｂが許可状態に切り換えられており、かつ、スライドスイッチ３４ｂが許可状態に切り換えられてから所定時間経過していない場合に、第２の動作制御情報は許可を示している。また、スライドスイッチ３４ｂが禁止状態に切り換えられているか、あるいは、スライドスイッチ３４ｂが許可状態に切り換えられてから所定時間経過している場合に、第２動作制御情報は禁止を示している。

【０１１８】セキュリティ情報のメンテナンス動作が禁止されていれば（ステップＣ１３のＮｏ）、アクセスポイント１０は上記メンテナンスコマンドを拒否する（ステップＣ１４）。これにより、どのような外部機器であっても、セキュリティ情報のメンテナンスを行うことはできない。

【０１１９】一方、セキュリティ情報のメンテナンス動作が許可されていれば（ステップＣ１３のＹｅｓ）、アクセスポイント１０は上記メンテナンスコマンドを実行する（ステップＣ１５）。その際、ＰＩＮコードの書き換えが行われた場合には（ステップＣ１６のＹｅｓ）、アクセスポイント１０はリンクテーブルＴ１のデータをすべて削除する（ステップＣ１７）。

【０１２０】このように、セキュリティ情報のメンテナンス動作が許可されている場合のみ、外部機器からコマンドを送って、ＰＩＮコードの書き換え等を行うことができる。したがって、普段はスライドスイッチ３４ｂの操作によりセキュリティ情報のメンテナンス動作を禁止しておけば、勝手にセキュリティ情報をアクセスすることはできないため、アクセスポイント１０のセキュリティを確保できる。

【０１２１】また、アクセスポイント１０の管理者がスライドスイッチ３４ｂを禁止状態に切り換えておくのを忘れたとしても、所定時間経過すると、スライドスイッチ３４ｂの状態に関係なく、セキュリティ情報のメンテナンス動作が自動的に禁止されるため、アクセスポイント１０のセキュリティを確保することができる。

【０１２２】さらに、ＰＩＮコードが変更された場合には不正アクセス者によるデータの改竄の可能性を考慮してリンクテーブルＴ１のデータをすべてクリアしておくことで、セキュリティをさらに強化することができる。リンクテーブルＴ１をクリアした場合には、すべての外部機器に対して再度ＰＩＮコードの入力を求めることになる。この場合、アクセスポイント１０で新たに設定されたＰＩＮコードを知らないユーザはアクセスポイント１０へ接続することはできないことになる。

【０１２３】（ｄ）接続時の認証エラー処理

次に、接続時の認証エラー処理について説明する。

【０１２４】図２０および図２１はアクセスポイント１０における接続時の認証エラー処理の動作を示すフローチャートである。なお、図２０および図２１はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。

【０１２５】今、外部機器であるパソコン１００のＩＤがリンクテーブルＴ１に登録されていないものとする。このパソコン１００から接続要求があると（ステップＤ１１）、アクセスポイント１０は認証エラーテーブルＴ２を参照する（ステップＤ１２）。認証エラーテーブルＴ２には、図１６に示すように、以前に認証エラーとなった機器のＩＤ等が登録されている。

【０１２６】この認証エラーテーブルＴ２にパソコン１００のＩＤが登録されていなかった場合には（ステップＤ１３のＮｏ）、アクセスポイント１０は通常通りＰＩＮコードによる認証を行う（ステップＤ１４）。そして、認証ＯＫであれば、つまり、パソコン１００が入力したＰＩＮコードがアクセスポイント１０のＰＩＮコードと一致すれば（ステップＤ１５のＹｅｓ）、アクセスポイント１０はパソコン１００の接続を許可する（ステ

ップＤ１６）。

【０１２７】一方、認証エラーであった場合、つまり、パソコン１００が入力したＰＩＮコードがアクセスポイント１０のＰＩＮコードと一致しなかった場合には（ステップＤ１５のＮｏ）、アクセスポイント１０はパソコン１００の接続を拒否する（ステップＤ１７）。その際、アクセスポイント１０はパソコン１００のＩＤを取得し、そのＩＤを認証エラーテーブルＴ２に登録すると共に、上記ＩＤに対応したエラー回数を初期値“１”とし、さらに、ＲＴＣ回路７６から現在の時刻を取得して、その時刻を最終接続時刻として登録する（ステップＤ１８）。

【０１２８】また、上記ステップＤ１３において、リンクテーブルＴ１に接続要求先のパソコン１００のＩＤが登録されていたとする。つまり、以前にパソコン１００から入力されたＰＩＮコードが正しくないとして拒否されていたとする。

【０１２９】このような場合において、アクセスポイント１０は、まず、認証エラーテーブルＴ２内のパソコン１００のＩＤに対応したエラー回数が所定回数を越えているか否かをチェックする（ステップＤ１９）。その結果、エラー回数が所定回数以内であれば（ステップＤ１９のＮｏ）、アクセスポイント１０は通常通りＰＩＮコードによる認証を行う（ステップＤ２０）。そして、認証ＯＫであれば、つまり、パソコン１００が入力したＰＩＮコードがアクセスポイント１０のＰＩＮコードと一致すれば（ステップＤ２１のＹｅｓ）、アクセスポイント１０はパソコン１００の接続を許可する（ステップＤ２２）。このとき、認証エラーテーブルＴ２からパソコン１００に関するデータを削除しておく（ステップＤ２３）。

【０１３０】一方、エラー回数が所定回数を越えている場合には（ステップＤ１９のＮｏ）、パソコン１００は不正アクセス者であると判断し、パソコン１００の接続を拒否する（ステップＤ２４）。その際、認証エラーテーブルＴ２内の当該パソコン１００のエラー回数を更新すると共に、ＲＴＣ回路７６から現在の時刻を取得して最終接続時刻として更新する（ステップＤ２５）。また、上記ステップＤ２１において認証エラーとなった場合にも同様にであり、接続の拒否と共に認証エラーテーブルＴ２内の当該パソコン１００に関するデータの更新を行う（ステップＤ２４、Ｄ２５）。

【０１３１】このように、ＰＩＮコードによる認証時に認証エラーとなった場合の回数をカウントしておき、同一機器の認証エラー回数が所定回数を超えた場合には当該機器の接続を完全に拒否することで、同じ機器が何度もＰＩＮコードを入力してアクセスポイント１０に不正にアクセスすることを防止して、アクセスポイント１０のセキュリティを強化することができる。

【０１３２】なお、上記所定回数は例えば５回程度が妥当であるが、その回数は予め決められていても良いし、アクセスポイント１０の管理者が任意に設定できるようにしても良い。

【０１３３】また、認証エラーテーブルＴ２に新たな機器のデータを登録する際に、認証エラーテーブルＴ２に空きがなければ（データ有無フラグがすべて有の状態）、最終接続時刻の最も古い機器のデータを認証エラーテーブルＴ２から削除して、そこに新たな機器のデータを登録する。このように、古いデータを削除することで、不揮発性メモリ７５に設けられる認証エラーテーブルＴ２の登録件数（図１６の例ではＭ件）の中で新たな接続相手を優先して認証エラー回数を効率的に管理でき、使い勝手を向上させることができる。

【０１３４】以上のように、アクセスポイント１０に設けられたスイッチの操作によりＰＩＮコードによる認証動作やセキュリティ情報のメンテナンス動作を禁止することで、外部からの不正なアクセスを防止してセキュリティを強化することができる。さらに、スイッチの状態に関係なく、所定時間経過後にはＰＩＮコードによる認証動作やセキュリティ情報のメンテナンス動作を自動的に禁止状態に切り換えることで、管理者がスイッチ操作を忘れたとしてもセキュリティを確保することができる。

【０１３５】また、同じ機器から不正なＰＩＮコードの入力が何度もあった場合に、以後、その機器の接続を完全に拒否することで、正しいＰＩＮコードを知らない者が不正アクセスを試みることを防止することができる。

【０１３６】また、不揮発性メモリ７５に設けられるリンクテーブルＴ１へのリンクキーの登録件数数が記憶可能な最大数に達した後、新たな接続相手とリンクキーを登録する場合には、一定の規則（接続時刻が古いものやアクセス頻度が低いものなど）に従って既に記憶されたリンクキーを削除してその領域に新たなリンクキーを登録することで、新たな接続相手を優先して、その以後の接続時におけるＰＩＮコード入力を不要にでき、使い勝手を向上させることができる。

【０１３７】また、アクセスポイント１０内のＰＩＮコードが変更された場合に、リンクテーブルＴ１に登録されている各機器のリンクキーのすべてを削除して、接続時に新たなＰＩＮコードの入力を要求するようにしたことで、セキュリティを強化することができる。

【０１３８】ところで、各機器に装着されるＢＴ－ＰＣカード２０にはＢＴモジュールのＩＤが登録されており、アクセスポイント１０にＢＴ－ＰＣカード２０が装着された場合、図１５に示すＣＰＵ７２はＢＴ－ＰＣカード２０に登録されているＩＤを機器固有の情報として、アクセスポイント１０内の不揮発性メモリ７５のＩＤ格納部７５ａに格納する。

【０１３９】ここで、ＣＰＵ７２がＰＣカードインターフェースとしてのコネクタ６０を介してＢＴ－ＰＣカー

ド２０が交換されたことを検知した場合、リンクテーブルＴ１のデータをすべて削除して、各機器が接続されたときに新たにリンクキーを作成し直すといった処理を行う。

【０１４０】これは、ＢＴモジュール（ＩＤを記憶している）がＰＣカードなどの交換可能なユニットで構成されていた場合に、ユーザの手違いで最初にアクセスポイント１０に装着されていたＢＴモジュールとは別のＢＴモジュールが装着される可能性があるためである。つまり、リンクキーはＩＤなどを元に作成されるものであるため、ＢＴモジュール交換前のＩＤで作成されたリンクキーをそのまま残しておくと、ＢＴモジュール交換後のＩＤによって作成されるリンクキーとの矛盾が生じ、外部機器との接続ができなくなる。このような不具合を解消するため、ＢＴモジュールが交換された場合には、現在リンクテーブルＴ１に登録されているデータをすべて削除して、各機器が接続されたときに新たにリンクキーを作成し直すといった処理を行う。

【０１４１】なお、本発明は、アクセスポイント１０から離れた場所にある外部機器から無線により不正アクセスする場合に特に有効であるが、アクセスポイント１０へのアクセス手段として必ずしも無線である必要はない。すなわち、例えば図１に示すアクセスポイント１０とパソコン１００とが通信ケーブルを介して接続されるようなシステムであっても、上記実施形態で同様の手法を適用することで不正アクセスを防止することができる。

【０１４２】また、上記実施形態では、公衆回線１１の接続機能を備えたアクセスポイント１０を例にして説明したが、無線等により他機器との接続を行うための通信機能を備えた機器であれば、そのすべての機器に本発明の手法を適用できるものである。

【０１４３】また、各機器に用いられる無線通信モジュールとしては、ＰＣカード等の交換可能なユニットで構成されている必要はなく、機器内に内蔵されているものであっても良い。

【０１４４】また、無線通信方式としては、Ｂｌｕｅｔｏｏｔｈに限らず、他の方式であっても良い。

【０１４５】要するに、本発明は上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態で示される全構成要件から幾つかの構成要件が削除されても、「発明が解決しようとする課題」で述べた効果が解決でき、「発明の効果」の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【０１４６】また、上述した実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フロッピー（登録商標）ディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリなどの記録媒体に書き込んで各種装置に適用したり、通信媒体により伝送して各種装置に適用することも可能である。本装置を実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【０１４７】

【発明の効果】以上詳記したように本発明によれば、スイッチの状態に応じて、特定の識別コードによる認証が禁止または許可される。したがって、上記特定の識別コードを不正に知り得たとしても、上記スイッチを直接に設定操作しない限り、本機器とのリンクを張ることができない。さらに、所定時間経過後は上記特定の識別コードによる認証が自動的に禁止されるため、管理者がスイッチを禁止状態に戻し忘れたとしてもセキュリティを確保できる。

【０１４８】また、他の機器との間で接続を行うための各種管理情報に対する変更操作がスイッチの状態によって禁止または許可される。したがって、他の機器の不正ユーザが本機器と接続できたとしても、上記スイッチを直接に設定操作しない限り、各種管理情報を勝手に変更することはできない。さらに、所定時間経過後は上記各種管理情報の変更が自動的に禁止されるため、管理者がスイッチを禁止状態に戻し忘れたとしてもセキュリティを確保できる。

【０１４９】また、所定回数を越えて認証エラーとなった機器からの接続要求が拒否されるため、同一機器からの不正な接続の試みを防止できる。

【０１５０】また、メモリの登録件数が一杯にある状態では、その中で接続の可能性の低いリンク情報が削除されて新たな機器のリンク情報が登録されるため、使い勝手を向上させることができる。

【０１５１】また、特定の識別コードが変更された場合にメモリ内のすべてのリンク情報が削除されるので、新たな識別コードを知らないユーザからの不正アクセスを防止できる。

【０１５２】また、交換可能な無線通信ユニットを備えた電子機器において、無線通信ユニットの交換があった場合に、メモリ内のすべてのリンク情報が削除されるので、交換前の無線通信ユニットの識別コードにより作成されたリンク情報と交換後の無線通信ユニットの識別コードにより作成されたリンク情報との矛盾をなくして、他の機器との接続ができなくなることを防止できる。

【図面の簡単な説明】

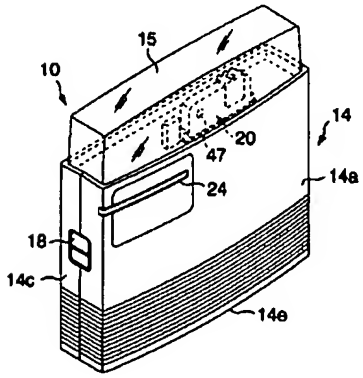
【図１】本発明の一実施形態に係る無線通信システムの外観構成を示す斜視図。

【図２】上記無線通信システムに用いられるアクセスポ

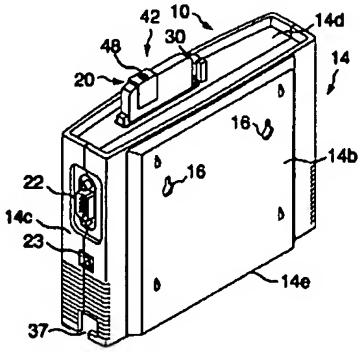
イントの分解斜視図。
【図３】上記アクセスポイントを縦置きで使用した状態を示す斜視図。
【図４】上記アクセスポイントの背面側を示す斜視図。
【図５】上記アクセスポイントを横置きで使用した状態を示す斜視図。
【図６】上記アクセスポイントの底面側を示す斜視図。
【図７】上記アクセスポイントに装着されるＢＴ－ＰＣカードの斜視図。
【図８】上記ＢＴ－ＰＣカードの分解斜視図。
【図９】上記無線通信システムの構成を示すブロック図。
【図１０】上記アクセスポイントに設けられたスライドスイッチの構成を示す図。
【図１１】上記アクセスポイントに設けられたロータリスイッチの構成を示す図。
【図１２】上記スライドスイッチと上記ロータリスイッチとの対応関係を示す図。
【図１３】上記アクセスポイントとＢＴ－ＰＣカードの回路構成を示すブロック図。
【図１４】上記アクセスポイントに外部機器として接続されるパソコンとＢＴ－ＰＣカードの回路構成を示すブロック図。
【図１５】上記アクセスポイントに設けられたリンクテーブルの構成を示す図。
【図１６】上記アクセスポイントに設けられた認証エラーテーブルの構成を示す図。
【図１７】上記アクセスポイントに設けられたスライドスイッチによる動作状態の切換え処理を示すフローチャート。
【図１８】上記アクセスポイントにおける外部機器との接続処理の動作を示すフローチャート。
【図１９】上記アクセスポイントにおけるセキュリティ情報のメンテナンス処理の動作を示すフローチャート。＊
＊【図２０】上記アクセスポイントにおける接続時の認証エラー処理の動作を示すフローチャート。
【図２１】上記アクセスポイントにおける接続時の認証エラー処理の動作を示すフローチャート。
【図２２】ＰＩＮコードによる認証動作を説明するための図。

【符号の説明】
１０…アクセスポイント
１２…モジュラケーブル
１４…機器本体
２０…ＢＴ－ＰＣカード
３４ａ、３４ｂ…スライドスイッチ
３５…ロータリスイッチ
４０…カード本体
４２…送受信部
４６…アンテナ部
４５、６０…コネクタ
７０…モデム部
７２…ＣＰＵ
７４…ＲＡＭ
７４ａ…第１の動作制御情報格納部
７４ｂ…第２の動作制御情報格納部
７４ｃ…基準時刻格納部
７５…不揮発性メモリ
７５ａ…ＩＤ格納部
７５ｂ…パスワード格納部
Ｔ１…リンクテーブル
Ｔ２…認証エラーテーブル
７６…ＲＴＣ回路
１００…パソコン
１１２…キーボード
１１６…ＬＣＤパネル
１２０…インターフェースコネクタ
１２２…ＣＰＵ

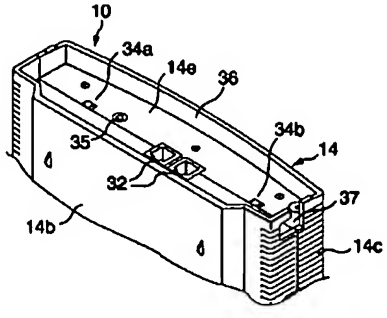
【図３】



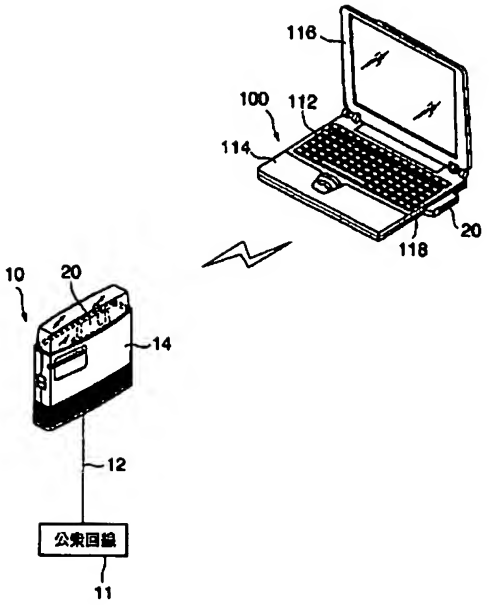
【図４】



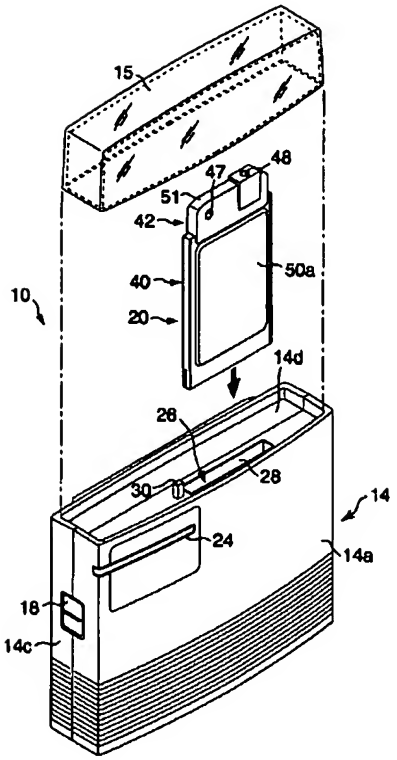
【図６】



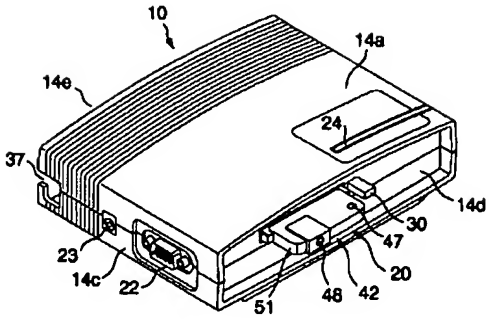
【図１】



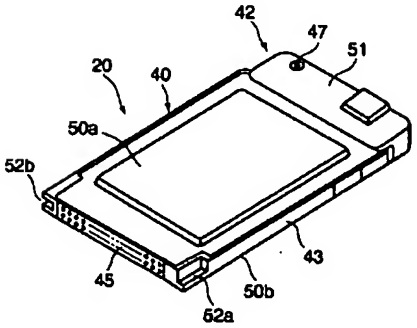
【図２】



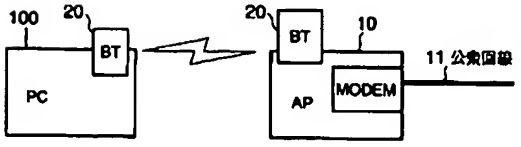
【図５】



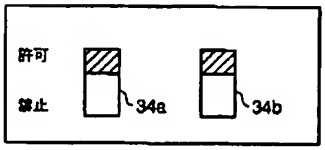
【図７】



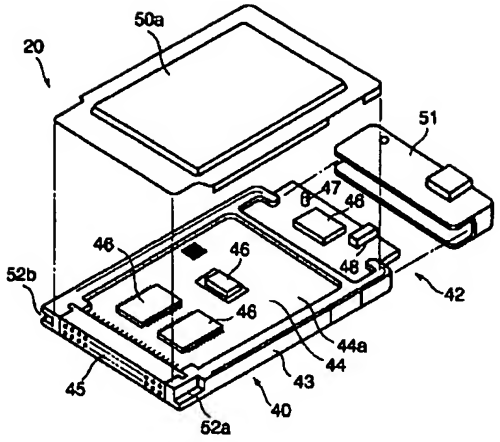
【図９】



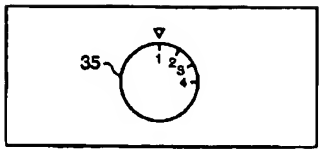
【図１０】



【図８】



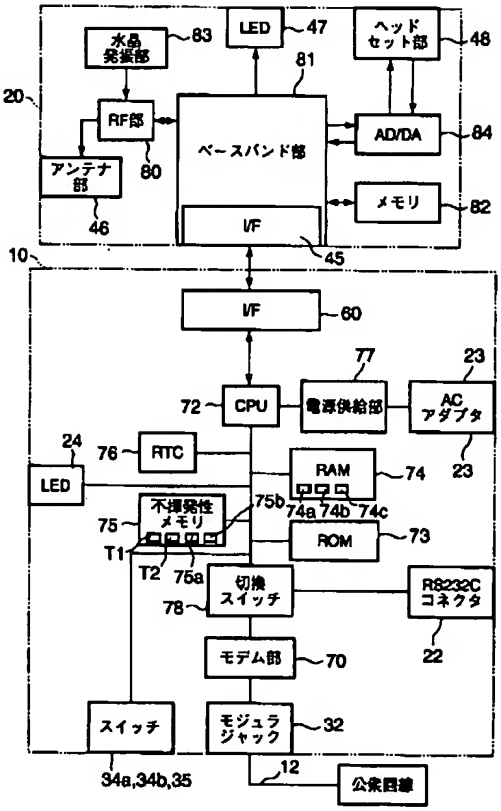
【図１１】



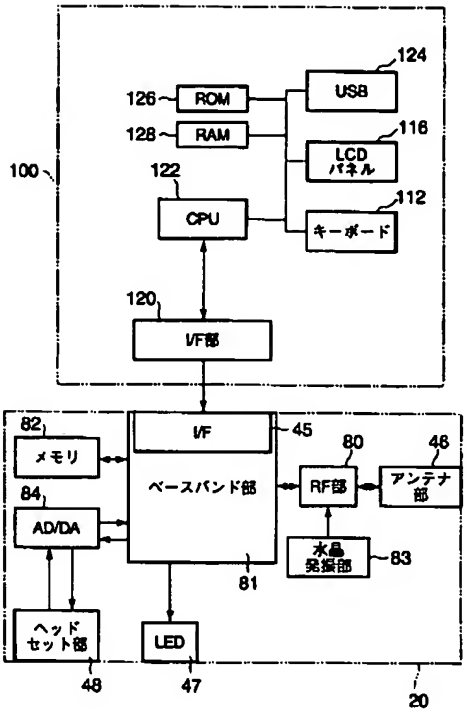
【図１２】

SW1	SW2	ロータリースイッチ
OFF	OFF	1
ON	OFF	2
OFF	ON	3
ON	ON	4

【図１３】



【図１４】



【図１５】

T1 リンクテーブル

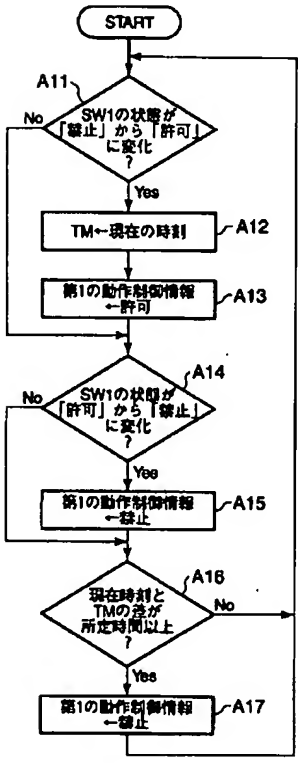
番号	ID (Hex)	リンクキー	最終接続時刻	データ有無フラグ
1	A36B35	XXXXXX	2000/07/20/12:00:10	有
2	4B3346	xxxxxx	2000/05/20/11:00:07	有
	⋮	⋮		
N-1	87647A	oooooo	2000/08/12/16:30:37	有
N	—	—		無

【図１６】

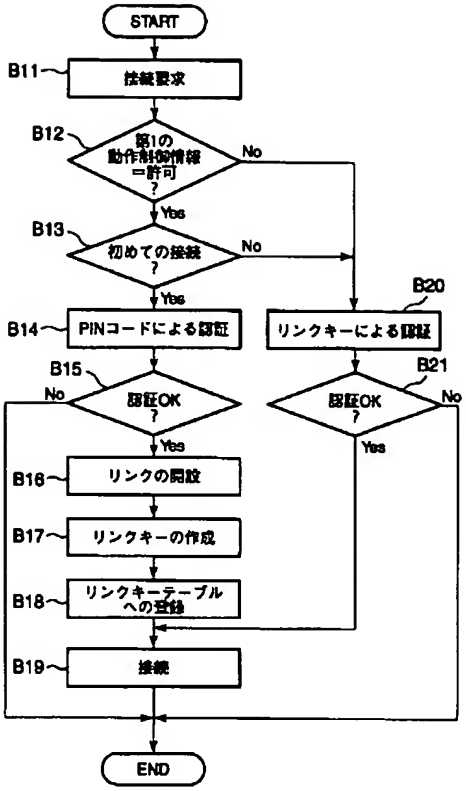
T2 認証エラーテーブル

番号	ID (Hex)	認証ｴﾗｰ回数	最終接続時刻	ﾃﾞｰﾀ有無ﾌﾗｸﾞ
1	A36B35	2	2000/07/20/12:00:10	有
2	4B3346	5	2000/05/20/11:00:07	有
	⋮	⋮		
M-1	87647A	1	2000/08/12/16:30:37	有
M	—	—		無

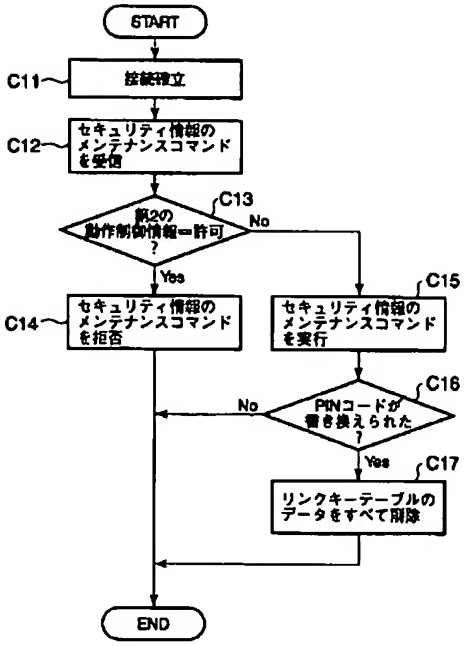
【図１７】



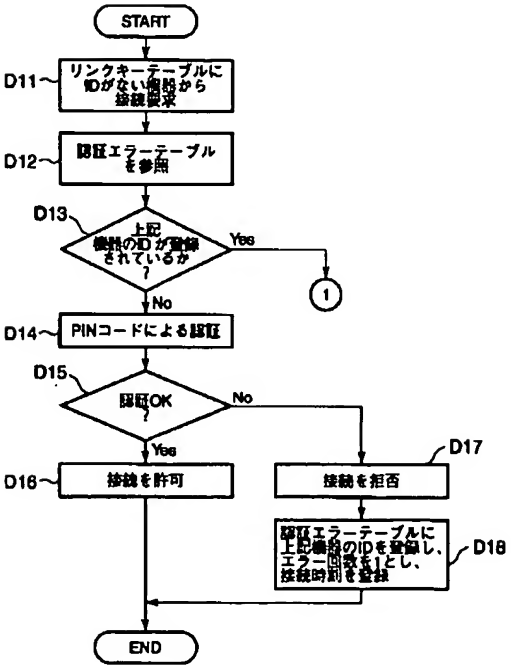
【図１８】



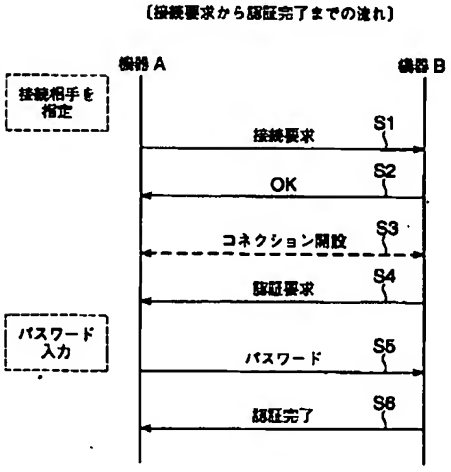
【図１９】



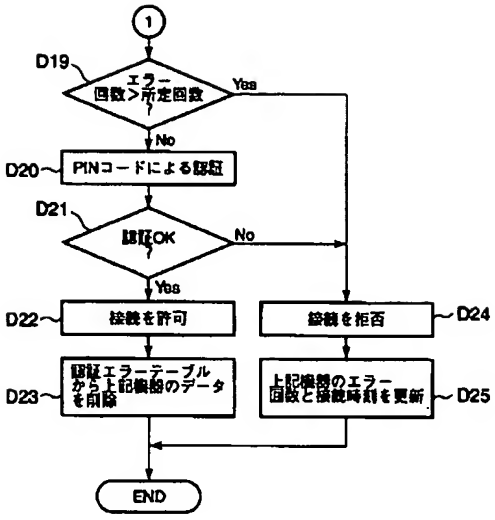
【図２０】



【図２２】



【図２１】


1
D19
エラー回数>所定回数
Yes
No
D20
PINコードによる認証
D21
認証OK
No
Yes
D22
接続を許可
接続を拒否
D24
D23
認証エラーテーブルから上記機器のデータを削除
上記機器のエラー回数と接続時刻を更新
D25
END